ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

Analýza a zhodnocení reálných hrozeb v kyberprostoru

Analysis and Evaluation of Real Threats in Cyberspace

Bakalářská práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Plánování a řízení krizových situací

Vedoucí práce: Ing. Melicharová Michaela

Neuman Lukáš

Kladno červenec 2017

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva Akademický rok: 2015/2016

Zadání bakalářské práce

Student: **Lukáš Neuman**

Obor: Plánování a řízení krizových situací

Téma: **Analýza a zhodnocení reálných hrozeb v kyberprostoru**

Téma anglicky: Analysis and Evaluation of Real Threats in Cyberspace

Zásady pro vypracování:

Cílem práce je průzkum informovanosti dospělé populace o nebezpečí, která je mohou ohrozit při využívání ICT technologií a internetu ve všech jeho podobách. Bakalářská práce bude zaměřena na běžné uživatele a nebude se zaměřovat na rizika ohrožující firemní sítě a veřejnou správu.
Teoretická část se bude věnovat odborným termínům, charakteristikám nejčastějších hrozeb ohrožujících běžné uživatele v kyberprostoru a právním předpisům souvisejícím s problematikou.
Praktická část bude zaměřena na dotazníkový průzkum informovanosti obyvatelstva v oblasti hrozeb kyberprostoru a formy využívání informačních technologií. Výstupem práce bude analýza výsledků průzkumu a stanovení doporučení pro zvýšení informovanosti obyvatel.

Seznam odborné literatury:

[1] KRÁL, Mojmír, Bezpečný internet: chraňte sebe i svůj počítač, ed. 1., Praha: Grada Publishing, a.s., 2015, 183 s., ISBN 978-80-247-5453-6
[2] JIROVSKÝ, Václav, Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství, ed. 1., Praha: Grada, 2007, 284 s., ISBN 978-80-247-1561-2
[3] LUDVÍK, Miroslav a ŠTĚDROŇ Bohumír, Teorie bezpečnosti počítačových sítí, ed. 1., Kralice na Hané: Computer Media, 2008, 98 s., ISBN 978-80-86686-35-6

zadání platné do: 11.09.2017

Vedoucí: Ing. Michaela Melicharová

....

vedoucí katedry / pracoviště děkan

V Kladně dne 23.02.2016

Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Analýza a zhodnocení reálných hrozeb v kyberprostoru vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně dne 18.05.2017

…….
podpis

Poděkování

Na tomto místě bych rád poděkoval vedoucí práce Ing. Michaele Melicharové za vedení této bakalářské práce a za její podnětné připomínky. Také bych chtěl poděkovat všem účastníkům průzkumu za jejich čas věnovaný vyplnění dotazníku.

Abstrakt

Cílem této bakalářské práce je určení největších hrozeb kyberprostoru ohrožujících běžné uživatele. V úvodu si definujeme, co vlastně slovo kyberprostor označuje, protože termín kyber- (kyberzločin, kyberkriminalita, apod.) je velice často užíván i v médiích, ale ne každý uživatel ví, co vlastně znamená. Dále jsou zde vyjmenovány největší hrozby. Nástin způsobů, jakým tyto hrozby uživatele ohrožují a základní jednoduché možnosti ochrany a obrany proti těmto hrozbám, které by měl bez větších obtíží zvládnout každý průměrný uživatel. Je zde také část, u které by se měl každý čtenář zamyslet, jestli sám sebe neohrožuje tím, co o sobě běžně uveřejňuje na různých sociálních sítích a v kyberprostoru obecně.

Praktická část je věnována průzkumu informovanosti uživatelů kyberprostoru o hrozbách, kterým je věnována teoretická část. Průzkum byl prováděn dotazníkovým šetřením pomocí nestandardizovaného dotazníku. Tento dotazník byl sestaven na základě stanovených hypotéz. Na základě odpovědí respondentů dotazníkového šetření jsou tyto hypotézy vyhodnoceny. Součástí praktické části práce je dále komparace získaných výsledků s výsledky získanými Šimoníkem (2013)(ŠIMONÍK, 2013) a zjištění, jak se za několik let změnila informovanost uživatelů o hrozbách kyberprostoru.

Klíčová slova

Kyberprostor, internet, bezpečnost, počítačové viry, malware.

Abstract

This bachelor thesis determines major cyberspace threats to common users. In the introduction we define the concept of cyberspace, because the cyber- prefix (cybercrime, cybergame, etc.) is used very frequently also in the media, although not every user is aware of its exact meaning. This part also enumerates the biggest threats. It presents the ways how these threats endanger the users, as well as basic possibilities of protection and defense against the threats, which every common user should master without any difficulties. Furthermore, it includes a food for thought: the readers should contemplate whether they do not endanger themselves by the material that they regularly publish on social networks and in cyberspace in general.

The practical part describes a survey of cyberspace users' awareness about the threats analyzed in the theoretical part. The survey was performed by means of a questionnaire research, using a non-standardized questionnaire. The questionnaire was drawn up based on pre-determined hypotheses. The hypotheses were subsequently assessed by comparing them with the answers given by the questionnaire respondents. The practical part of the thesis also compares the results with those received by Šimoník (2013) and studies how the users' awareness about cyberspace threats has changed over the past years.

Key words

Cyberspace, Internet, safety, computer viruses, malware

Obsah

ÚVOD

Co je to vlastně kyberprostor? Existuje mnoho definic, ale vlády a vědci nejsou schopni se shodnout na jediné. Podle jedné z definic je to synonymum pro internet, podle Kohoutka (2008) *„je to virtuální svět vytvořený moderními technologickými prostředky.“* (KOHOUTEK, 2008) Podle starší definice Sterlinga (1982) *„je kyberprostor místo, kde se vyskytují lidé bez fyzických těl. Klasický příklad zní: Když zvednete telefon a vytočíte telefonní číslo vašeho kamaráda, kde se bude odehrávat váš rozhovor? Bude to ve vašem sluchátku? V jeho telefonním přístroji? V drátech, které vás spojují? Ne. Tento hovor se bude odehrávat v kyberprostoru.“* (STERLING). Jedna z posledních a zřejmě nejpřesnější je definice kyberprostoru, kterou sestavil tým na Scuola Superiore Sant'Anna v Pise v roce 2014: *„Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery, atd..), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data.“* (MAYER, a další, 2014).

V současnosti kyberprostor užívá téměř každý člověk v západní civilizaci, ale málokdo si uvědomuje rizika a nebezpečí, která s sebou toto médium přináší pro běžné uživatele. V teoretické části této práce budou uvedeny největší a nejčastější hrozby, které ohrožují běžné uživatele s uvedením jednoduchých opatření, jak se jednotlivým hrozbám bránit. V praktické části bude proveden průzkum informovanosti uživatelů o těchto hrozbách a jeho analýza, případné návrhy na možnost zlepšení informovanosti o těchto hrozbách.

1 CÍLE PRÁCE

Teoretická část práce obsahuje informace o hrozbách, které nejčastěji ohrožují všechny uživatele internetu. Viry, trojské koně, červi, phishing, pharming, sociální inženýrství a další dále zmíněné hrozby ohrožují všechny, ať se jedná o privátní uživatele, nebo o firmy a instituce. Nebudeme se věnovat hrozbám, ohrožujícím především firmy a instituce, které privátní uživatele spíše omezují, ale firmy a instituce přímo poškozují jako např. útoky typu DDoS.

Cílem praktické části práce je potvrzení nebo vyvrácení navržených hypotéz. Pro zhodnocení hypotéz budeme používat výsledky získané pomocí nestandardizovaného anonymního dotazníku, který byl mezi respondenty distribuován v elektronické podobě pomocí sociálních sítí. Zaměření dotazníku bylo směřováno na informovanost uživatelů ohledně hrozeb, které je ohrožují z kyberprostoru. V další části bude provedena komparace námi získaných výsledků s výsledky získanými Šimonikem (2013)(ŠIMONÍK, 2013)

Cíle práce:

- Přinést základní informace o běžných hrozbách plynoucích z kyberprostoru.
- Přinést základní informace, jak se těmto hrozbám bránit.
- Zmapování informovanosti obyvatel o kybernetických hrozbách, které je ohrožují.
- Potvrzení nebo vyvrácení stanovených hypotéz, které se zabývají informovaností o hrozbách kyberprostoru.
- Komparace a zhodnocení vývoje výsledků dotazníkového šetření s podobným dotazníkovým šetřením Šimonik (2013).

2 BEZPEČNOST INTERNETU U NÁS

Nad bezpečností internetu u nás dohlíží CSIRT.CZ, který je provozován sdružením CZ.NIC od ledna 2011, na základě veřejnoprávní smlouvy uzavřené mezi sdružením CZ.NIC a NBÚ, který je gestorem problematiky kyberbezpečnosti.

Dle statistiky zobrazené pod obrázkem 1, je velice dobře vidět, jaké typy útoků nejvíce ohrožují kyberprostor na území české republiky (CSIRT.CZ je národní tým, který má na starosti veškeré problémy týkající se počítačových sítí pouze na území České republiky).

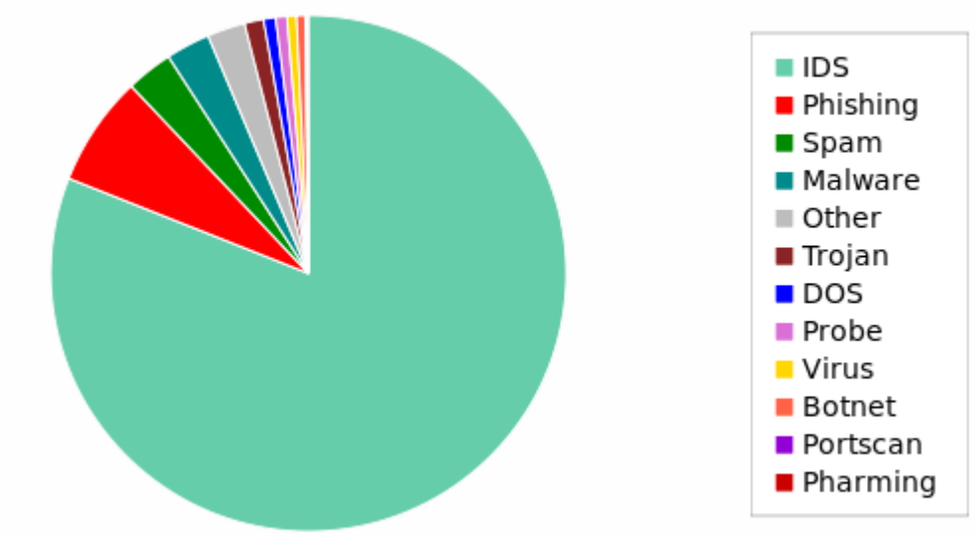
V posledních 5 letech se objevily incidenty typu IDS, které dříve nebyly identifikovány (tedy ne že by se objevily z ničeho nic). Jedná se o detekci nestandardního chování počítačových systémů. Jedná se o platformu pracující s IP adresami, které nejsou využívány a tváří se, že na těchto adresách běží funkční systém. V případě kontaktu na takovouto adresu se systém snaží udržet útočníka co nejdéle z toho důvodu, aby neškodil jinde.(CSIRT, 2015)

Další a pro uživatele jeden z nejvýznamnějších typů útoku je phishing. Tyto útoky jsou evidovány od roku 2008 a jejich množství vzrůstalo. V roce 2008 bylo těchto útoků 65 a v dalších letech se množství útoků zvyšovalo až k hranici 370 útoků za rok. K těmto počtům jsme se dostali v letech 2014, 2015 a 2016, kdy podle CSIRT.CZ bylo těchto útoků podstatě stejně (368 v roce 2014, 367 v roce 2015 a 363 v roce 2016). Dle statistiky za první 2 měsíce roku 2017 se zdá, že počet útoků v tomto roce bude zřejmě vyšší než v předchozích letech.

Obrázek 1 - Statistika incidentů národního týmu CSIRT za jednotlivé roky, zdroj: CSIRT.CZ

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	sum
IDS				491	3924	2121	2380	3771	9944	2551	25182
Phishing	65	220	209	144	159	175	368	367	363	85	2155
Spam	47	28	103	26	43	73	159	108	290	35	912
Malware	53	134	121	10	20	45	117	240	104	16	860
Other	1	5	13	62	14	75	102	264	181	22	739
Trojan	66	6	26	5	5	12	56	90	79	28	373
DOS	2	4	2	2	68	72	32	37	12	4	235
Probe		3	14	25	12	26	86	42	13		221
Virus		84	99								183
Botnet		3	46	5	8	15		4	71	15	167
Portscan	10	4	1	6	1	3	2	5	6	1	39
Pharming							18	3	2	1	24
sum	244	491	634	776	4254	2617	3320	4931	11065	2758	31090

Obrázek 2 – celkový počet incidentů v letech 2006 - 2017, zdroj: CSIRT.CZ



Také další typy útoků nás ohrožují. Jsou jimi například, spam, malware, viry, trojští koně, sociální inženýrství, phishing, pharming. V této práci se budeme těmto hrozbám věnovat v tom ohledu, že bude vysvětleno, co která hrozba znamená a stručný nástin toho, jak se které hrozbě bránit.

2.1 Nebezpečný software

Veškerá zařízení, která jsou připojena do internetu (PC, smartphony, tablety), jsou neustále ohrožována nebezpečími, jejichž množství roste každým dnem. Nebezpečný software se označuje také jako malware, jehož autoři mají různé pohnutky. Někteří jen jako dokázání si „já na to mám“, ale velká část toho nejnebezpečnějšího malwaru vznikla z důvodu obohacení autora na úkor obětí. Většina lidí považuje veškerý škodlivý software za viry, ale malware se dělí do tří velkých skupin.

2.1.1 Viry

Nazývají se viry, protože se projevují podobně jako biologické viry. Počítačové viry, stejně jako ty biologické, škodí hostiteli. Mají schopnost se reprodukovat a dále se šířit. Různé viry škodí různým způsobem, některé jsou téměř neškodné, pouze obtěžují uživatele, jiné poškozují data, další blokují paměť a ty nejnebezpečnější jsou schopné smazat obsah pevného disku počítače a tím jej vyřadit z provozu (např. virus Michelangelo, který se spouštěl 6. března v den narození Michelangela Buonarrotiho a přepsal část pevného disku náhodnými znaky). Existují také viry schopné poškodit hardware (např. virus Černobyl, který se spouštěl 26. dubna v den výročí výbuchu JE Černobyl a dokázal smazat flash paměť ve které je uložen BIOS počítače).

Podle schopností se viry dají rozdělit na:

- Bootviry - napadá pouze boot sektor, kde je uložena zaváděcí část OS. Po spuštění PC je vir aktivní v paměti RAM při vložení dříve převážně diskety, dnes spíše USB flash disku, nebo externího disku, dojde k jeho replikování na toto médium a při vložení takovéhoto infikovaného média do jiného PC k další replikaci viru do zatím neinfikovaného PC.
- Rezidentní viry – při spouštění systému je tento typ viru načten do paměti RAM, kde běží skrytě, kontroluje spouštěné aplikace a používané soubory, které průběžně infikuje.
- Stealth viry – jedná se o schopnost viru, kdy se vir schovává a maskuje před kontrolou antivirovým programem. Provádí to tak, že buď podává falešnou informaci, nebo předkládá originální informaci, kterou si pro případ kontroly zálohoval.
- Multipartní viry – napadají jak spustitelné soubory tak i boot sektory disku. Většinou je to FAT tabulka u starších systémů, u novějších systémů je to část disku, kde jsou uloženy informace o rozdělení disku.
- Makroviry – jejich cílem jsou soubory dokumentů např. sady MS Office (Word, Excel), ve kterých jsou použita makra. Makra jsou v podstatě relativně jednoduché programy, které jsou vytvářeny uživateli pro zjednodušení úkolů, které se často a rutinně opakují. Mnoho uživatelů vytváří makra pomocí nástroje pro záznam makra a neuvědomuje si, že se jedná o velmi propracovaný programovací jazyk, ve kterém se dají vytvářet i viry. Musí se jednat o makra, která se spustí automaticky, nezávisle na uživateli (např. při otevření souboru, nebo při uzavření). Pokud se například v aplikaci MS Word povede infikovat šablonu NORMAL.DOT, přebírá okamžitě kontrolu nad aplikací, protože tato šablona je načítána automaticky při spuštění.

- Polymorfní viry – při své replikaci se částečně mění kód tohoto typu viru, proto je složitější je odhalit antivirovým programem.
- Souborové viry – cílem těchto virů jsou spustitelné soubory (*.com, *.exe, *.dll, *.vbs), tyto viry se ještě rozdělují:
    - Přepisující virus – replikuje se místo původního obsahu. Z tohoto důvodu je původní soubor nenávratně poškozen a nepracuje tak, jak by měl. Jedná se o dost nápadné chování, které se některé viry pokoušely maskovat chybovým hlášením.
    - Link virus – dosti inteligentní funkce viru, kdy se virus pouze připojí k původnímu souboru bez poškození jeho funkčnosti. Zpravidla se nejprve provedla akce viru a poté se následně spustily instrukce, které měly proběhnout podle původního souboru.
    - Doprovodný virus – existoval dříve, kdy využíval funkce starých OS, vytvořil kopii souboru zpravidla s příponou *.exe, kdy nově uložený soubor měl příponu *.com. Při pokusu o spuštění původního souboru OS přednostně spustil soubor *.com. Nejprve se provedly instrukce viru a pak až následně byl spuštěn původní soubor.

Většina virů využívá více z těchto schopností, a ne jen jednu, takže existuje například rezidentní polymorfní stealth virus apod. Kombinace těchto schopností využívají viry k tomu, aby byly hůře odhalitelné antivirovými programy.

Výše jsou popsány schopnosti virů. Nyní se stručně podíváme na to, jak se nejčastěji viry projevují. Zde jsou ty nejvýznamnější projevy virů (jejich vliv na počítač, OS):

- Blokace místa – vir je v podstatě skupina instrukcí, tedy musí zabírat nějaké místo na disku, v případě boot virů a rezidentních virů i v operační paměti (tato vlastnost virů je při jejich malé velikosti a při velikostech dnešních pamětí a pevných disků téměř zanedbatelná).
- Zpomalení systému – další celkem logická vlastnost virů je to, že ke své aktivitě (aktivace, šíření) potřebuje virus část systémových prostředků (čas, kdy využívá procesor). Tyto jeho aktivity probíhají skrytě a uživateli se jeví jako zpomalení PC.
- Narušení stability OS a aplikací – u virů, které napadají soubory, může dojít k narušení integrity aplikace a nekompatibility se systémem, nebo periferiemi. Následkem mohou být havárie systému či aplikací, nebo zamrznutí celého PC (toto může být způsobeno virem, ale nemusí).
- Vyskakovací okna a jiné evidentní projevy – je vlastnost některých virů, které dělají pravý opak toho co většina, a to že různými způsoby na sebe upozorňují. Zobrazují uživateli různá vyskakovací okna žádající interakci, například napsání určitého slova. Jiný zase každý den v určitou dobu přehraje určitý zvuk, píseň, apod. Relativně málo nebezpečné, ale spíše otravné.
- Odcizení a možnost zneužití dat- některé z velmi nebezpečných virů sbírají data v infikovaném počítači a tato soukromá data mohou odesílat pomocí internetu kamkoliv po světě. Mohou třeba data postupně šifrovat. Pokud se k nim uživatel pokusí dostat, automaticky je dešifrují, aby uživatel nic nepoznal. Ve chvíli, kdy má dostatek požadovaných dat nebo v určitý den, najednou data zablokuje a odešle pryč.
- Poškození a zničení dat – jiné viry data v infikovaném počítači mohou mazat nebo náhodně přepisovat, buď okamžitě po infikování, nebo jen v určitý den v roce,

nebo postupně šifrovat data do dosažení určité hranice, kdy uživatel nic nepozná. Při dosažení dané hranice vir zablokuje šifrovaná data, zničí se, a s tím i dešifrovací klíč. Do této skupiny by se daly zařadit i viry, které zašifrují data a následně požadují odeslání financí na dané číslo účtu, jinak zůstanou data zašifrována a tudíž nepoužitelná. (KRÁL, 2015)(JIROVSKÝ, 2007)(MIKLÁŠ, 2013)(HÁK, 2005)(URBAN)

2.1.2 Trojští koně

Tato hrozba je pojmenována podle historické pověsti z dob trojské války. Zdálo se, že Řecko-Trojská válka bude nekonečná pro neproniknutelnost trojských hradeb. Proto se řečtí velitelé uchýlili ke lsti a vytvořili obrovskou figuru koně, coby dar bohům, ve které bylo ukryto několik řeckých vojáků. Poté zdánlivě opustili pobřeží Troji. Obránci města v euforii z konce války vtáhli dar za hradby města, aniž by jej jakkoli prozkoumali. V noci, když celé město spalo, zmoženo oslavami konce války, opustili Řekové svůj úkryt a vpustili vrátivší se spolubojovníky do města. To byl konec slavného města Troji.

Toliko historická vsuvka a nyní zpět k současnosti. Trojský kůň z pohledu počítačové terminologie je program bez schopnosti sebe-replikace (nemůže sám sebe rozšířit), ale spoléhá na hloupost a zvědavost uživatelů, aby se infiltroval do PC. Jedná se o soubory, které útočník nejčastěji pošle mailem, nebo jsou na určitých serverech ke stažení. Mají pro uživatele zajímavé a lákavé názvy (např. se tvářily ve starších systémech jako spořič obrazovky, což je také spustitelný soubor), nebo se tváří jako užitečný soubor. Velice často jsou trojští koně ukryti na stránkách s pornografií a nelegálním softwarem. Ve chvíli, kdy je takovýto škodlivý program spuštěn, začne vykonávat svoji škodlivou činnost. Existuje několik skupin trojských koní, které si dále popíšeme.

- Password-stealing trojští koně tzv. PWS) – nebo také keylogger – typ trojského koně, který ukládá klávesy stisknuté na klávesnici PC a následně odesílá na určené místo (adresu). Tímto způsobem mohou být získány přihlašovací jména a hesla na různé internetové stránky a různé účty (internetové bankovnictví, emailový účet apod.).
- Dropper – jedná se o trojského koně, který po spuštění vpustí do počítače další trojské koně nebo viry, které má uloženy ve svém kódu.
- Downloader (trojandownloader) – obdoba předchozího trojského koně, jen s tím rozdílem, že tento má v sobě uloženy pouze URL adresy, ze kterých po spuštění stahuje další škodliviny, jako jsou trojští koně a viry. V některých případech mohou být na cílových URL používány skripty, které způsobí stažení různých škodlivých kódů v závislosti na konkrétní situaci. V některých případech může po stažení první dávky škodlivých kódů dojít ke spuštění stahování dalších a dalších virů a trojských koní a používaný počítač se tak stane fakticky nepoužitelným pro svoji pomalost.
- Destruktivní trojští koně – tento trojský kůň po svém spuštění začne ničit data, šifrovat data, nebo rovnou naformátuje celý disk.
- Backdoor – tzv. zadní vrátka. Jedná se o zvláštní skupinu trojských koní, kteří po spuštění umožní autorovi přístup do napadeného PC pomocí tzv. zadních vrátek (jedná se v podstatě o vzdálenou správu PC, ale bez možnosti ovlivnění uživatelem tohoto PC).
- Proxy trojský kůň – někteří trojští koně napadají proxy server a odtud odesílají spam. Už z principu proxy je nemožné identifikovat skutečného odesílatele takovéto pošty. (KRÁL, 2015)(JIROVSKÝ, 2007)(MIKLÁŠ, 2013)(BITTO, 2005)(KOCMAN, a další, 2005)

2.1.3 Worms (Červi)

Za své pojmenování vděčí zřejmě spisovateli Johnu Brunnerovi, který v roce 1975 vydal knihu The Shockwave Rider (Jezdec na rázové vlně), kde byl použit název Tapeworm pro program schopný samostatného šíření, který měl na pokyn svého tvůrce vyřadit celou telefonní síť.

Z historického hlediska byl první červ vytvořen v laboratořích firmy XEROX, jehož úkolem bylo sledovat vytíženost jednotlivých počítačů připojených k firemní síti a v případě nečinnosti jim přidělit úkol. Tímto bylo dosaženo optimálního využití výpočetního potenciálu celého výpočetního střediska.

Historicky prvním červem, který způsobil problémy, byl tzv. Morrisův červ (vytvořil ho Robert T. Morris). Mělo se jednat o neškodný program, určený ke změření rozsahu internetu, ale díky chybně naprogramovanému mechanismu svého šíření způsobil 2. listopadu 1988 tehdejšímu internetu obrovské problémy, kdy došlo k zahlcení téměř celého tehdejšího internetu.

V současnosti jsou jako červi chápany všechny škodlivé programy a části kódu, které jsou na rozdíl od virů schopny se sami šířit pomocí internetu (vir o existenci sítě nemá ponětí a není schopen ji využít, naproti tomu červ si existenci sítě „uvědomuje“).

Červi se dále dělí podle svých vlastností:

- E-mailoví červi – jedná se o soubory, které jsou šířeny pomocí e-mailu. Ve chvíli, kdy je takovýto soubor spuštěn uživatelem, červ se aktivuje, prozkoumá uložené e-mailové adresy a rozešle svoji kopii na nalezené adresy a zároveň začne provádět svoji škodlivou činnost. Typicky se počítač stane součástí botnetu (botnet

je skupina počítačů napadených červem, která na pokyn tvůrce může být použita k rozesílání spamu, nebo k DDoS útokům).

- Internetoví červi – využívají všechny dostupné prostředky infikovaného počítače ke skenování ostatních počítačů v síti a vyhledávání jejich bezpečnostních chyb. Pokud nějakou nalezne a je ji schopen využít, napadne tento počítač a pokud se mu povede proniknout přes zabezpečení takového počítače, nainstaluje se zde a provádí dále svojí činnost (typicky opět botnet). Jeho velké nebezpečí je v tom, že ke svému šíření nepotřebuje žádnou akci uživatele.
- Share červi – tito červi využívají servery určené ke sdílení dat, kam nakopíruje sám sebe. V kombinaci se zajímavým názvem může být dost pravděpodobně mnohokrát stažen a spuštěn. Následně je infikovaný počítač typicky připojen k botnetu, nebo ovládán autorem červa. (KRÁL, 2015) (JIROVSKÝ, 2007) (MIKLÁŠ, 2013)(URBAN)(KOCMAN, a další, 2005) (ROUSE, 2016)(KASPERSKY LAB)

2.1.4 Další škodlivý software

V této části bude zmíněn další škodlivý software, který uživatele, až na výjimky, spíše obtěžuje, ale je zde výjimka v podobě dialerů. Tyto škodlivé programy mohly hlavně v dřívějších dobách vytáčeného internetu uživatele připravit o nemalé částky.

- Spyware – jedná se o software, který bývá velmi často šířen pomoci sharewarových, freewarových programů jako jejich součást. Tyto části programů sbírají o uživateli statistická data. Například navštěvované internetové stránky, nainstalované programy, jak často je počítač využíván apod. Tyto údaje odesílají tvůrci tohoto softwaru údajně za účelem přesného cílení reklamy, ale nikde není řečeno, že se tato data nedají zneužít.(MICROSOFT)

- Adware – jedná se spíše o obtěžující, než o vysloveně škodlivý software. Konkrétně obtěžuje reklamami v různých podobách. V některých případech se jedná pouze o reklamu, někde po straně mimo hlavní okno programu, kterého je součástí. V jiných případech se jedná o vyskakující okno, které musíme zavřít. V některých případech jde zavřít až po několika vteřinách. Je to daň za to, že některé programy můžeme používat zdarma, jindy jen proto, abychom se dostali k tomu, co potřebujeme najít na internetu.(KASPERSKY LAB)
- Dialer – jednalo se o problém zvláště v dřívějších dobách, kdy byl internet poskytován přes telefonní linku (tzv. vytáčený internet). Dialer je program, který přesměroval relativně levné výchozí telefonní číslo na jiné a velice často velmi drahé telefonní číslo. Nejběžnější částky se pohybovaly kolem 60 kč/min, ale byly i případy, kdy se jednalo o stovky kč/min. Toto se dělo buď skrytě pomocí ActiveX prvků (tedy hlavně přes internet explorer), např. návštěvou nevhodné internetové stránky, nebo v jiných případech se tak dělo se souhlasem uživatele, ale který nemusel vědět o tom, co vlastně potvrzuje. Uživatel kolikrát věděl pouze o tom, že se jedná údajně o výhodnou službu, ale cena nebyla uvedena, nebo byla v neviditelné části obrazovky apod.(KOCMAN, a další, 2005)

2.2 Ochrana

Proti všem těmto způsobům napadení a ohrožení počítače se dá bránit několika relativně jednoduchými věcmi, které si krátce probereme.

- Antivirový program – jedná se o program, který pokud úmyslně nevypneme, nebo to neudělá některý z výše uvedených škodlivých programů sám, běží neustále na pozadí počítače v operační paměti a vyhodnocuje chod počítače. Při své běžné činnosti a běžných testech antivirový program hledá jen jemu známé viry. Z toho plyne potřeba pravidelné aktualizace antivirového programu. Pokud

není aktuální databáze virů, tak antivirový software netuší, co má vlastně hledat a viry se mohou nerušeně prohánět počítačem. Pouze pokud je aktivována možnost hloubkového testu, má antivir určitou šanci, že se mu podaří najít nějaký podezřelý řetězec v testovaném souboru a vyhodnotit jej jako vir. Tuto možnost mnoho uživatelů nepoužije, protože je časově náročnější a mnozí o ní ani nevědí. Nyní by si mohl někdo říci, že více antivirových programů má větší šanci nalézt něco podezřelého, ale opak je pravdou. Mnohdy se navzájem antiviry označí za viry, nebo se může stát, že pokud narazí na skutečný vir, dojde mezi nimi „k boji o něj“ a může vše skončit kolapsem systému. Tedy naše doporučení zní- jeden kvalitní antivirový program s pravidelnými aktualizacemi by měl běžet v každém počítači, zvláště v takovém, který je připojen k internetu. Na trhu existuje mnoho kvalitních antivirových programů. Většina velkých a známých firem vytvářejících ty nejkvalitnější antiviry poskytuje základní antivirový software zdarma. Jedná se o základní diagnostiku a ochranu PC v reálném čase, ale bez dalších prémiových funkcí.

- Aktuálnost operačního systému – když byla řeč o aktualizování databáze antivirového programu, je na místě zmínit i aktuálnost operačního systému. Průběžně s tím, jak tvůrci virů a jiného škodlivého softwaru hledají nedostatky operačních systémů, zvláště těch od firmy Microsoft, tak vývojáři operačních systémů, vytváří tzv. záplaty, aby tyto odhalené chyby opravily. Tudíž neaktuální systém rovná se zjednodušená možnost infekce počítače. Vzhledem k náročnosti této akce je velice snadné udržovat operační systém stále aktuální. U operačních systémů Windows lze nastavit tak, že není potřeba žádný zásah uživatele (pouze po dokončení aktualizace je většinou potřeba počítač restartovat). Na toto je uživatel upozorněn a lze v případě nevhodnosti odložit na příhodnější čas.
- Antispyware – software vyhledávající a odstraňující spyware a adware. U mnoha antivirových programů bývá součástí placené verze. U verzí zdarma je

třeba zvláštní program, který toto obstarává. Je možné nalézt mnoho programů zdarma.

- Firewall – doslovně přeloženo ohnivá zeď, která může být buď softwarová (případ domácností a menších firem) nebo hardwarová (případ velkých firemních sítí). Řídí síťovou komunikaci na základě předem definovaných pravidel. Pokud se přes firewall pokusí projít žádost o odesílání dat, nebo o přístup z vnější sítě, která neodpovídá pravidlům, může být buď automaticky odmítnuta, nebo upozorněn uživatel a je na něm, jak rozhodne o takovéto komunikaci (zda ji povolí nebo zamítne). Jak firewall tak antivir by měly být aktivní již v okamžiku, kdy je počítač připojen do sítě.(KASPERSKY LAB)
- Wi-Fi – v současnosti je naprosto běžné mít v téměř každé domácnosti wi-fi router. Bylo by možné namítnout, že toto nesouvisí s nebezpečnými programy, ale jen na půl. Pokud se bude někdo chtít infiltrovat do domácí sítě, může využít nechráněnou wi-fi a vypustit do této sítě některé nepříjemné červy a trojské koně a problémy jsou hned na světě. Proto by každý domácí router měl mít alespoň základní zabezpečení, kterým je požadavek hesla pro připojení a změna přednastaveného hesla pro administraci takovéhoto routeru. Je pravdou, že tato ochrana před zkušeným hackerem neuspěje na moc dlouho, ale proč útočníkovi zjednodušovat přístup do naší domácí sítě.(KOCMAN, a další, 2005)(BITTO, 2006)

Toto jsou asi tak základní informace pro zabezpečení domácího počítače před škodlivým softwarem.

2.3 Další hrozby pro uživatele

Předchozí kapitola se věnovala nebezpečným programům, které ohrožují naše domácí počítače a nyní se podíváme na další možnosti jak ohrozit uživatele s pomocí jeho interakce.

2.3.1 Spam

Spam jako takový není přímo nebezpečným, ale je více než obtěžujícím. Určitě každému z nás, kdo používáme nějakou dobu stejný e-mailový účet, se stalo, že mu na něj začaly chodit nevyžádané reklamní e-maily a nikdo netušíme, kde odesílatel vzal naší e-mailovou adresu. Je to jednoduché. Při téměř každé registraci na nějakou internetovou stránku jsme nuceni zadat e-mailovou adresu. Tyto servery vám často začnou posílat reklamní e-maily, případně mohou tyto adresy poskytnout (prodat) dále, což je sice v rozporu se zákonem 101/2000 Sb. zákon o ochraně osobních údajů, ale je to těžko prokazatelné. Nebo si u těchto serverů někdo zaplatí za reklamu a my máme rázem mailovou schránku plnou nevyžádané pošty. Většina e-mailových serverů umožňuje označit adresu odesílatele jako spam a dále se ke zprávám z této adresy chová odpovídajícím způsobem. Tyto filtry ale využívají i svoje databáze spam adres a nepříjemnější stránkou spamu pak může být zařazení očekávané zprávy mezi spam a možnost o takovouto zprávu přijít.

2.3.2 Pharming

Pharming, česky překládán také jako pharmaření, je velmi nebezpečná technika útoku, kterou nemusí odhalit ani odborník, nebo jen velmi těžce. Jedná se o typ útoku, kdy útočník napadne tzv. DNS server. Úkolem DNS serveru je vzájemný převod doménového jména (např. www.seznam.cz) na IP adresu (77.75.77.53), která jednoznačně definuje konkrétní server. Pokud útočník napadne takovýto server a změní zde tyto údaje, pak se může po zadání běžné adresy internetového bankovnictví (např. www.servis24.cz pro internetové bankovnictví České spořitelny a.s.) klientovi zobrazit jakákoliv stránka zvolená útočníkem (typická stránka, která je k nerozeznání od skutečné stránky internetového bankovnictví). Po zadání přihlašovacích údajů jsou tyto údaje uloženy útočníkem a následně pro snížení nápadnosti může dojít k přihlášení na reálné stránky banky, aniž by měl uživatel šanci cokoli zaregistrovat. Účinná obrana

proti této technice je velmi těžká a pro běžné uživatele v podstatě neexistuje. Možností obrany je to, že některé banky pro přihlášení k internetovému bankovnictví požadují zadání kódu, který stránky odešlou na předem sjednaný mobilní telefon. Případně jsou tyto kódy požadovány pro většinu změn na stránkách banky nebo pro transakce. (BEDNÁŘ, 2007)(BITTO, 2005)(MITTELBACH, 2008)(KASPERSKY LAB)

2.3.3 Sociální inženýrství

Je to technika získávání informací nebo také prospěchu s využitím nejslabšího článku bezpečnosti v oboru počítačů, a tím je člověk s dostatečnými přístupovými právy. Základní myšlenkou sociálního inženýrství je, proč se namáhat se složitým a velmi často časově náročným prolamováním potřebných hesel, když jej mohu získat přímo od toho, kdo jej zná.

Asi nejznámějším sociotechnikem na světě je Kevin Mitnick, který jako první tento termín definoval. Stal se nechtěně mediální hvězdou a jedním z nejhledanějších lidí v historii FBI. Hrozil mu trest ve výši několika set let vězení za ilegální průniky do stovek počítačových systémů velkých korporací. Na jeho obranu považujeme za nutné říci, že v napadených počítačích nikdy nezničil žádná data, ani ze svých akcí neměl žádný finanční prospěch. V letech 1982 až 2000 strávil mnoho měsíců pod soudním dohledem, několikrát byl zavřen ve vězení a 6 měsíců i ve středisku pro léčbu závislostí (byl soudně uznán závislým na počítačích). Byl také odsouzen k zákazu používání telefonů a počítačů na 3 roky. Poté co byl propuštěn v prosinci 2000 naposledy z vězení, naprosto změnil svůj život a přešel na druhou stranu. V současnosti je z něj světově uznávaný expert na zabezpečení počítačových systémů.

Sociální inženýrství využívá různé techniky, ale všechny spoléhají jen na jedno - na lidskou důvěřivost a hloupost. Neb jak řekl Albert Einstein *„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.“*.(EINSTEIN) Jaké konkrétní techniky a postupy sociotechnici používají? Často ty nejjednodušší metody jsou ty nejúčinnější. Ve své výpovědi před kongresem USA jak získával hesla a citlivé údaje od firem, Kevin Mitnick uvedl: *„Představil jsem se jako někdo jiný a prostě jsem o ně požádal.“*(KUNEŠ, 2012) Pro útoky typu sociálního inženýrství slouží nejčastěji internet, nebo telefon, ale je možné informace získat i tzv. tváří v tvář, ale o toto se pokoušejí jen ti nejzkušenější sociotechnici.

Pokud útočník oběť dobře zná, je někdy možné odvodit přístupová hesla. Mnoho lidí totiž často používá různá data ze svého života, nebo jména dětí, domácích mazlíčků, oblíbených knižních, nebo filmových postav a jejich různé kombinace.

Je několik základních metod, které sociotechnici užívají, pokud útočí na konkrétní firmu:

- Útočník zcela bez váhání zkusí požádat o přihlašovací údaje. Jedná se o naprosto primitivní pokus, ale i takové někdy vyjdou.
- Útočník předstírá, že je nadřízeným oběti a oběť je jedinou osobou na světě, která mu může pomoci (například se nachází mimo firmu na jednání a nutně potřebuje informaci např. o programech používaných pro vzdálený přístup, jeho konfiguraci apod.). Zaměstnanec samozřejmě velice rád pomůže svému „šéfovi“.
- Další možností je, že útočník vybere účet nového zaměstnance, nebo méně šikovného v oblasti výpočetní techniky a předstírá nedostatek znalostí pro první přihlášení k firemnímu účtu, nebo předstírá ztrátu či zapomenutí svých přihlašovacích údajů a nutně potřebuje pracovat na svém projektu. Oběť často pomůže kolegovi poskytnutím svých přihlašovacích údajů (musíme si přeci

pomáhat). Nebo pokud je obětí někdo na administrátorské pozici, může vygenerovat k účtu nové heslo, případně pomoci s „prvním přihlášením“.

- Často používanou metodou je, že útočník předstírá, že je zaměstnancem podpory a nutně potřebuje k ověření přihlašovací jméno a heslo zaměstnance. Méně proškolení a nepozorní zaměstnanci někdy na takovouto vějičku skočí.
- V neposlední řadě je užívána možnost, kdy útočník nachystá takovou situaci, aby jej oběť sama požádala o pomoc, v domnění, že útočník je zaměstnanec firmy z oddělení informatiky.
- Další z často používaných technik využívajících spoléhání se na lidskou zvědavost, je „zapomenutý“ CD-ROM, nebo DVD s nějakým zajímavým názvem (domácí video, nebo videa z dovolené apod.) na vhodném místě, kde tento nosič bude spolehlivě nalezen. Na takovémto nosiči mohou být, mimo zmíněného, uloženy také různé viry, případně trojští koně, kteří se po vložení nosiče do mechaniky skrytě nainstalují a začnou okamžitě plnit svoji činnost. Takovýmto nosičem může být i USB-flash disk nebo paměťová karta

V naší republice je asi nejběžnější formou sociálního inženýrství phishing, česky označován jako rhybaření. Je to podvodná technika, která je používána pro získání citlivých údajů, nebo finančního prospěchu. Jejím základem je buď e-mail, nebo aplikace pro přímou komunikaci tzv. instant messaging (např. ICQ, Skype, facebook messenger a další), kdy se útočník vydává za představitele banky, úředníka státní správy nebo administrátora a požaduje po oběti, aby se přihlásila na stránku, která je k nerozeznání podobná třeba internetovému bankovnictví. Uživatel zde zadá své uživatelské jméno a heslo, které může být následně útočníkem zneužito. Aby oběti nebylo nápadné, že se nic neděje, může falešná stránka mimo uložení přihlašovacích údajů následně provést přesměrování na oficiální stránku a uživatele automaticky přihlásit, ten poté opravdu nic nepozná. Ochranou proti této technice je pouze nedůvěřovat žádné zprávě, do které

odesílatel přiloží odkaz a po adresátovi chce, aby se na něj přihlásil. Je bezpečnější použít odkaz, který je běžně používán uživatelem pro přihlášení (jistota oficiální stránky). Některé banky v reakci na tyto podvodné maily zavedly možnost ověření klienta pomocí přihlašovací SMS zprávy, doručované na předem zvolený mobilní telefon, bez které není možné se přihlásit, nebo potvrzení transakcí pomocí takovéto zprávy. Mimoto na mnoha serverech se objevuje upozornění typu: naši administrátoři po vás nikdy nebudou požadovat přihlašovací údaje.

Dalším typem útoků sociotechniků může být využití buď nátlaku, nebo soucitu k získání finančního prospěchu. Tento typ útoků se v ČR již také několikrát objevil. Jedná se o různé zprávy, které buď upozorňují na nezaplacené půjčky, faktury apod. a požadují po adresátovi okamžité zaplacení, nebo bude přistoupeno buď k soudnímu řešení, nebo již dokonce k exekuci. Často se stává, že tyto zprávy jsou psány s chybami, což by mělo potencionální oběť varovat. Obdobou těchto útoků mohou být podobné, kdy útočník se tváří, že nemá například dostatek peněz na cestu domů, protože ten s kým se měl sejít, nepřišel, nebo žádosti o přispění na nějaký dobročinný účel. Tento typ útoků může probíhat jak v kyberprostoru, tak i v reálném světě. S největší pravděpodobností se v reálném světě setkáme s útoky, které spoléhají na dobrotu obětí.

Sociotechnici využívají důvěřivost, nevědomost a hloupost lidí, proto účinnou obranou je nedůvěřovat podobnému jednání. Případně si ověřovat údaje a žádosti jinou cestou. Nevýhodou je, že sociotechnici často lidi udržují ve stresu tvrzením o nedostatku času. V časovém presu mnoho lidí jedná jinak než v klidu, kdy by si mohli vše dobře rozmyslet. Proto je lepší se uklidnit a nenechat se nijak tlačit do něčeho do čeho nechceme.(MITNICK, a další, 2003)(PŘIBYL, 2007)(VÍTEK, a další, 2004)(CHRISTENSEN, 1999)(ROUSE, 2016)(ŠTĚDROŇ, a další, 2008)

2.3.4 Uživatelé jako hrozba sami sobě

V této části bych se rád zmínil o fenoménu, kterým jsou sociální sítě a u nás zejména Facebook. Zde by se dalo říci, že se uživatelé dělí do 3 skupin. První skupina jsou tací, kteří na Facebooku o sobě nesdělí nikomu téměř nic. Mnoho lidí pro svoji anonymitu nepoužívá třeba ani skutečné jméno, ale pouze nějakou přezdívku. Druhou skupinou jsou běžní uživatelé, kteří sem tam o sobě něco sdělí, používají skutečná jména, ale přemýšlí, co o sobě napíší. A poslední takovou skupinou, která je pravým opakem té první skupiny, jsou lidé, kteří o sobě sdělují neustále a téměř v přímém přenosu vše, co kdy a kde dělají. Domníváme se, že toto může být za určitých okolností velice nebezpečné. Jako příklad můžeme uvést příspěvek, který bude veřejný a bude obsahovat sdělení typu: „V pátek odjíždíme na deset dní na dovolenou do Itálie. Už se tak těším, jak si odpočinu.“ Toto sdělení může být velmi nebezpečné, protože tím dáváme celému světu vědět, že náš byt bude prázdný, a tudíž ideální typ na vykradení. Stejně tak může být nebezpečné se touto cestou chlubit novými věcmi apod.

Proti této hrozbě existuje jen jedna ochrana, dobře si předem rozmyslet, co o sobě člověk chce opravdu napsat. Je bezpečnější například zahraniční dovolenou nedeklarovat dopředu, ale pokud máme tu potřebu, tak se pochlubit až po návratu z dovolené, kdy už je každému zloději jedno, že byt byl prázdný 10 dní. V tuto chvíli už toho nijak nemůže využít.(ŠTĚDROŇ, a další, 2008)

3 DOTAZNÍKOVÉ ŠETŘENÍ

V této kapitole jsou prezentovány výsledky provedeného průzkumu. V první části se nacházejí stručné informace o provedeném dotazníkovém šetření

3.1 Popis výzkumu

Pro tuto bakalářskou práci byla zvolena metoda výzkumu formou dotazníkového šetření, k čemuž byl použit nestandardizovaný anonymní dotazník (viz. Příloha 1), který byl distribuován elektronickou formou pomocí sociálních sítí a e-mailu. Výzkumné šetření probíhalo od 1. 1. 2017 do 31. 3. 2017.

Jako výzkumný nástroj byl použit vytvořený dotazník, který je složen z 2 částí. V první části se nachází základní informace o respondentech, v části druhé se nachází vlastní výzkum. Otázky byly vytvořeny tak, aby odpovídaly cílům práce a předem stanoveným hypotézám. V první části otázek byl zjišťován věk, pohlaví a vzdělání respondentů. Tato část obsahuje 3 otázky. Vlastní dotazník se skládá celkem ze 14 otázek zaměřených na informovanost ohledně jednotlivých hrozeb kyberprostoru.

Dotazník byl tvořen 13 uzavřenými otázkami, u kterých si respondenti mohli zvolit jednu z předem definovaných odpovědí (u jedné otázky byla možnost zvolit více možností). Otázka č. 10 byla otevřená, kde respondenti odpovídali svými slovy. Tato otázka byla dostupná pouze části respondentů, podle toho jak odpověděli na otázku č. 9. Ti, kteří odpověděli záporně, přeskočili v dotazníku rovnou na otázku 11.

3.2 Hypotézy

Hypotéza 1

Předpokládáme, že více než 70 % respondentů používá minimálně jednu sociální síť.

Hypotéza 2

Předpokládáme, že více než 50 % respondentů ví, co znamená pojem sociální inženýrství.

Hypotéza 3

Předpokládáme, že více než 50 % respondentů se setkalo s phishingem.

Hypotéza 4

Předpokládáme, že více než 75 % respondentů používá antivirový program.

Hypotéza 5

Předpokládáme, že více než 70 % respondentů se setkalo ve svém počítači s počítačovým virem.

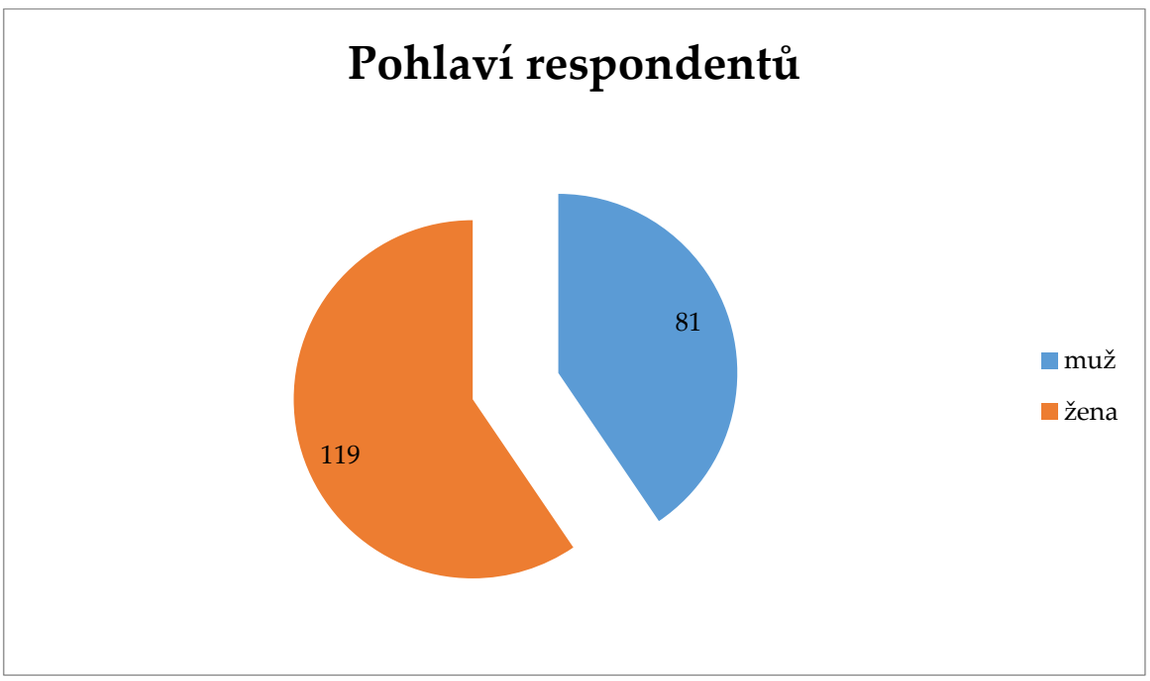
3.3 Prezentace výsledků

Dotazník byl šířen pomocí sociálních sítí a e-mailu, z tohoto důvodu je skupina respondentů velmi rozličná a nestejnorodá, není zde zcela rovné zastoupení pohlaví. S ohledem k této formě síření dotazníku jsou respondenti rozdílného věku a vzdělání.

Otázka č. 1 - Pohlaví respondentů

- Muž
- Žena

Graf 1 - Pohlaví respondentů



Tabulka 1 - Pohlaví respondentů

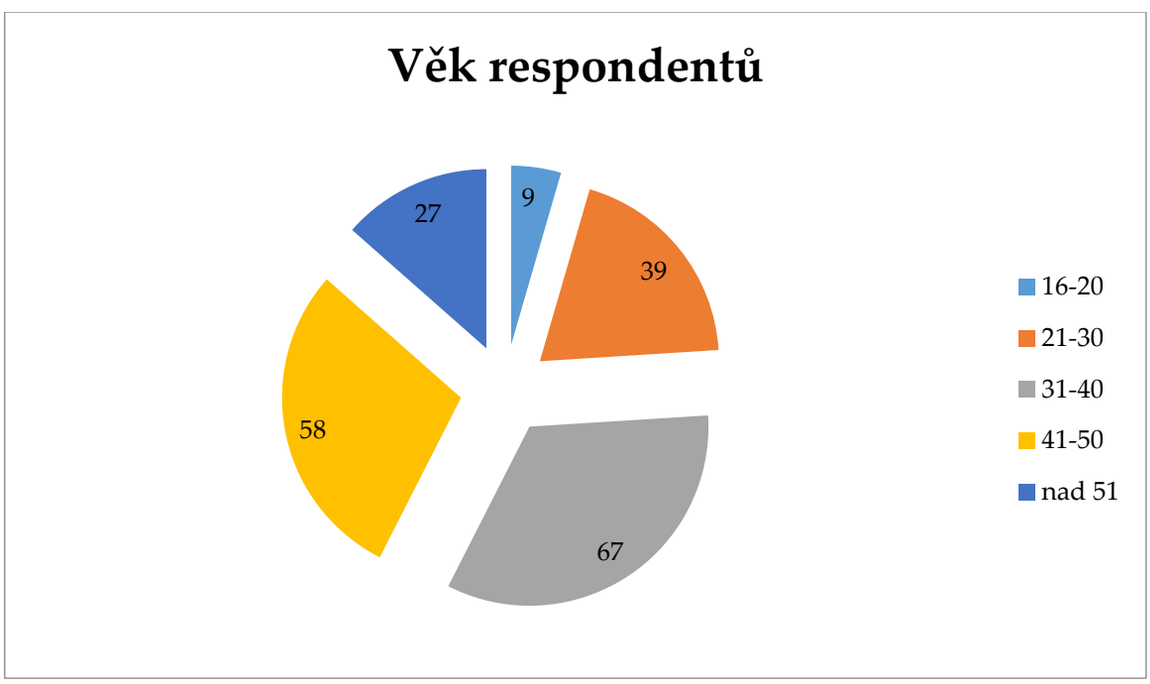
pohlaví	počet respondentů	podíl v %
Muž	81	40,5 %
Žena	119	59,5
Celkem	200	100 %

Jak je uvedeno před prezentací jednotlivých otázek, skupina respondentů byla zvolena zcela náhodě, z tohoto důvodu je zastoupení pohlaví nerovnoměrné.

Otázka č. 2 - Věk respondentů

- 16-20 let
- 21-30 let
- 31-40 let
- 41-50 let
- nad 51 let

Graf 2 - Věk respondentů



Tabulka 2 - Věk respondentů

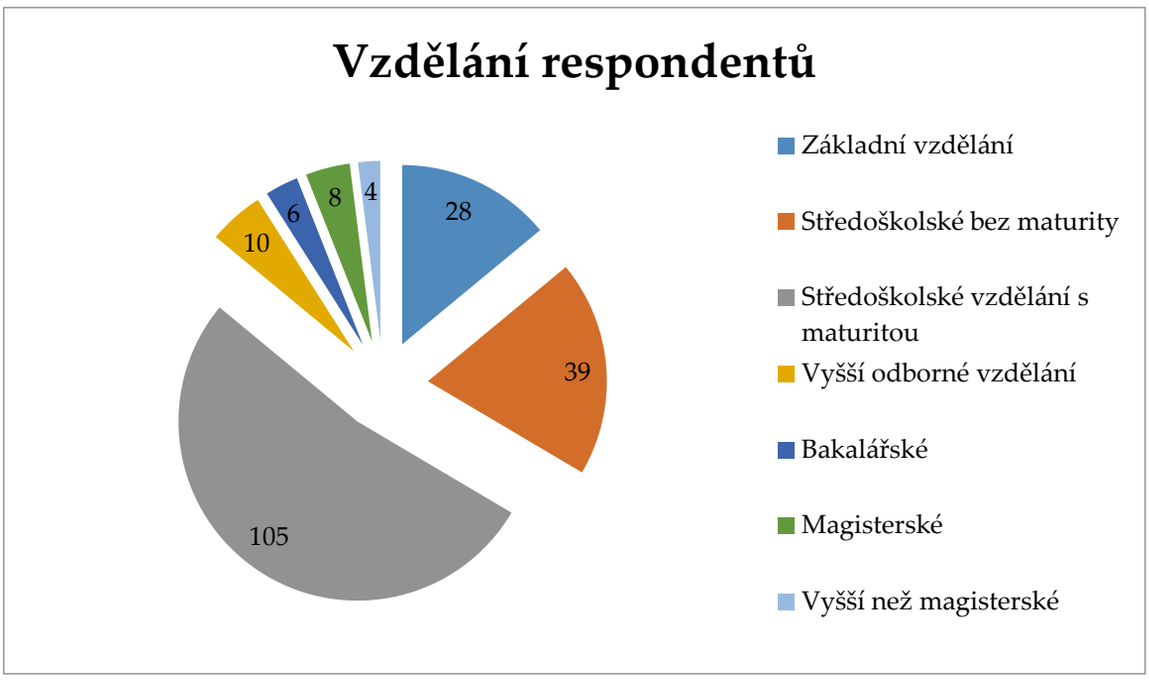
Věk respondentů	počet respondentů	podíl v %
16-20	9	4,5 %
21-30	39	19,5 %
31-40	67	33,5 %
41-50	58	29 %
Nad 51	27	13,5 %
Celkem	200	100 %

Věkové rozložení respondentů je pro potřeby tohoto průzkumu odpovídající. Má jít o zmapování informovanosti v dospělé populaci. Je dobře, že více než 95 % respondentů je ve věku nad 20 let. Vzdělávání této skupiny již bylo z většiny ukončeno, a pokud se tato skupina nebude chtít vzdělávat sama, již ji k tomu nikdo nedonutí.

Otázka č. 3 - Vzdělání respondentů

- Základní vzdělání
- Středoškolské bez maturity
- Středoškolské vzdělání s maturitou
- Vyšší odborné vzdělání
- Bakalářské
- Magisterské
- Vyšší než magisterské

Graf 3 - Vzdělání respondentů



Tabulka 3 - Vzdělání respondentů

vzdělání respondentů	počet respondentů	podíl v %
Základní vzdělání	28	14 %
Středoškolské bez maturity	39	19,5 %
Středoškolské vzdělání s maturitou	105	52,5 %
Vyšší odborné vzdělání	10	5,0 %
Bakalářské	6	3,0 %
Magisterské	8	4,0 %
Vyšší než magisterské	4	2,0 %
Celkem	200	100 %

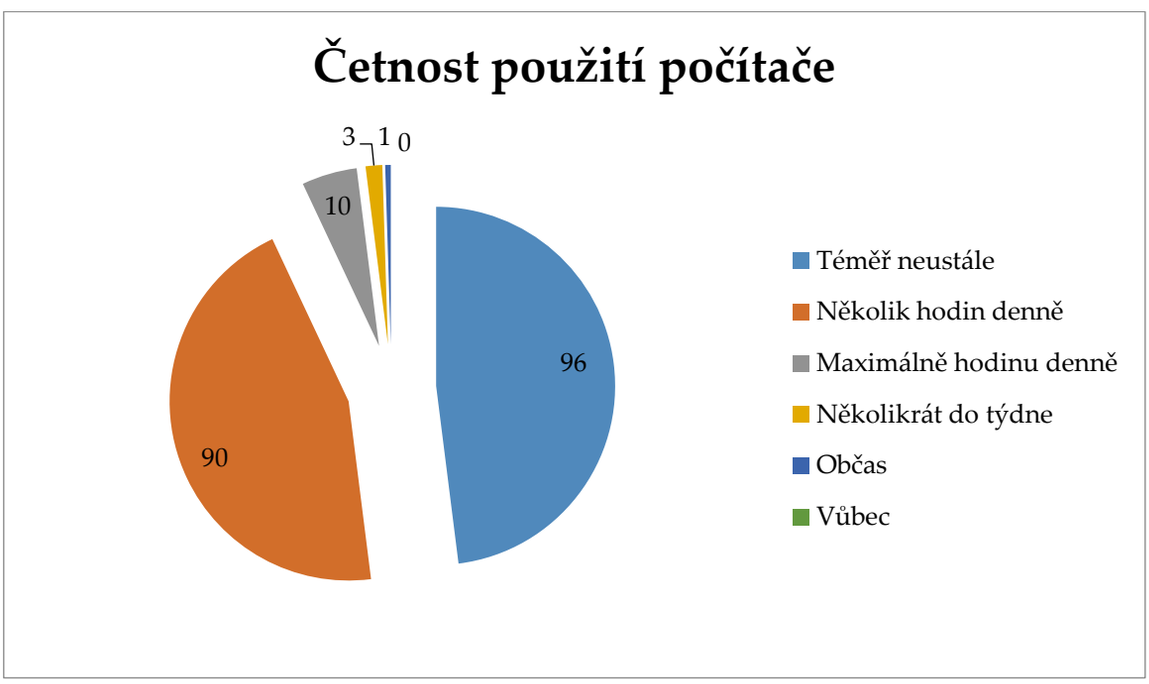
Když bylo vyhodnoceno zastoupení dosaženého vzdělání v jednotlivých věkových skupinách, pokud tedy vynecháme skupinu do 20 let, ve které je výskyt vyššího než středoškolského vzdělání možný jen naprosto výjimečně. Bylo zjištěno, že ve skupinách 21-30, 31-40, 41-50 je úroveň vzdělání rozvržena relativně stejnoměrně. Nejvíce se v každé z těchto skupin vyskytuje středoškolské s maturitou přibližně v 60 % odpovědí.

Ve skupině nad 51 let toto již neplatí. Zde je zastoupeno středoškolské s maturitou, středoškolské bez maturity a základní naprosto shodně přibližně v 33 %. Zbývající 1 % zbývá na vysokoškolské vzdělání.

Otázka č. 4 - Jak často používáte počítač, tablet, mobilní telefon nebo nějaké jiné zařízení s přístupem k internetu?

- Téměř neustále
- Několik hodin denně
- Maximálně hodinu denně
- Několikrát do týdne
- Občas
- Vůbec

Graf 4 - Četnost použití počítače



Tabulka 4 - Četnost použití počítače

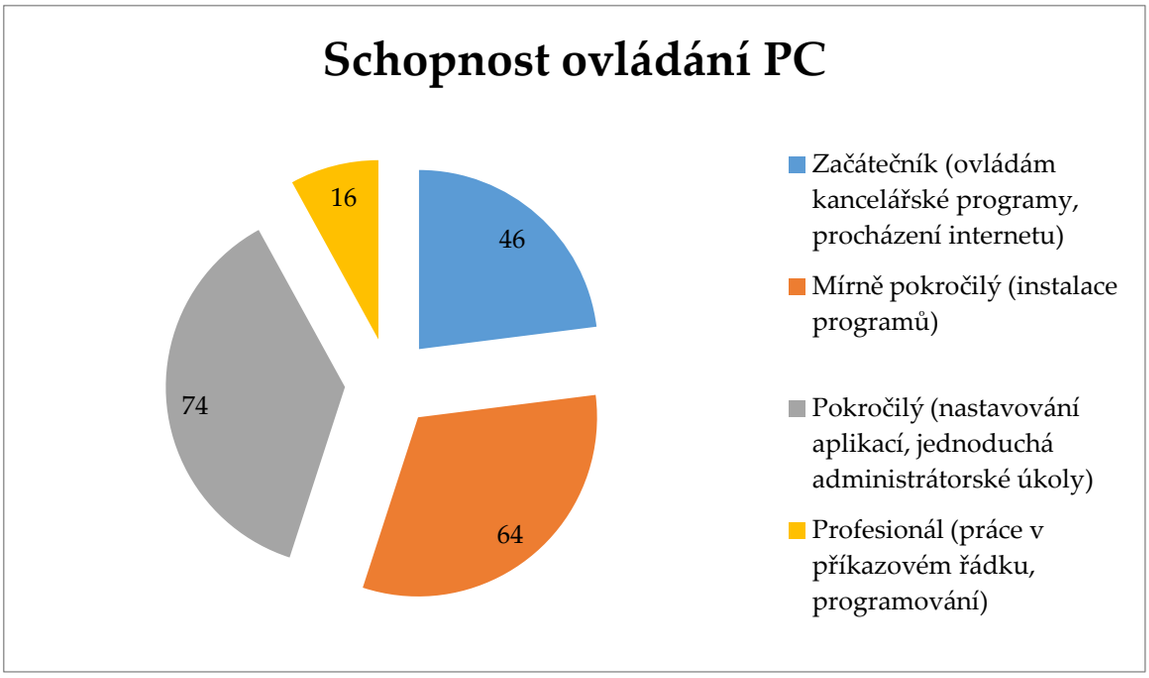
Použití počítače	počet respondentů	podíl v %
Téměř neustále	96	48 %
Několik hodin denně	90	45 %
Maximálně hodinu denně	10	5 %
Několikrát do týdne	3	1,5 %
Občas	1	0,5 %
Vůbec	0	0,0 %
Celkem	200	100 %

Tato otázka měla přiblížit, jak moc je naše civilizace závislá na počítačích. Celých 93 % respondentů uvedlo, že počítač používá minimálně několik hodin denně. A pouze 2 % respondentů uvedlo, že počítač používají maximálně několikrát týdně.

Otázka č. 5 - Za jak schopného se považujete při práci na PC?

- Začátečník (ovládám kancelářské programy, procházení internetu)
- Mírně Pokročilý (instalace programů)
- Pokročilý (nastavování aplikací, jednoduchá administrátorské úkoly)
- Profesionál (práce v příkazovém řádku, programování)

Graf 5 - Schopnost ovládání PC



Tabulka 5 - Schopnost ovládání PC

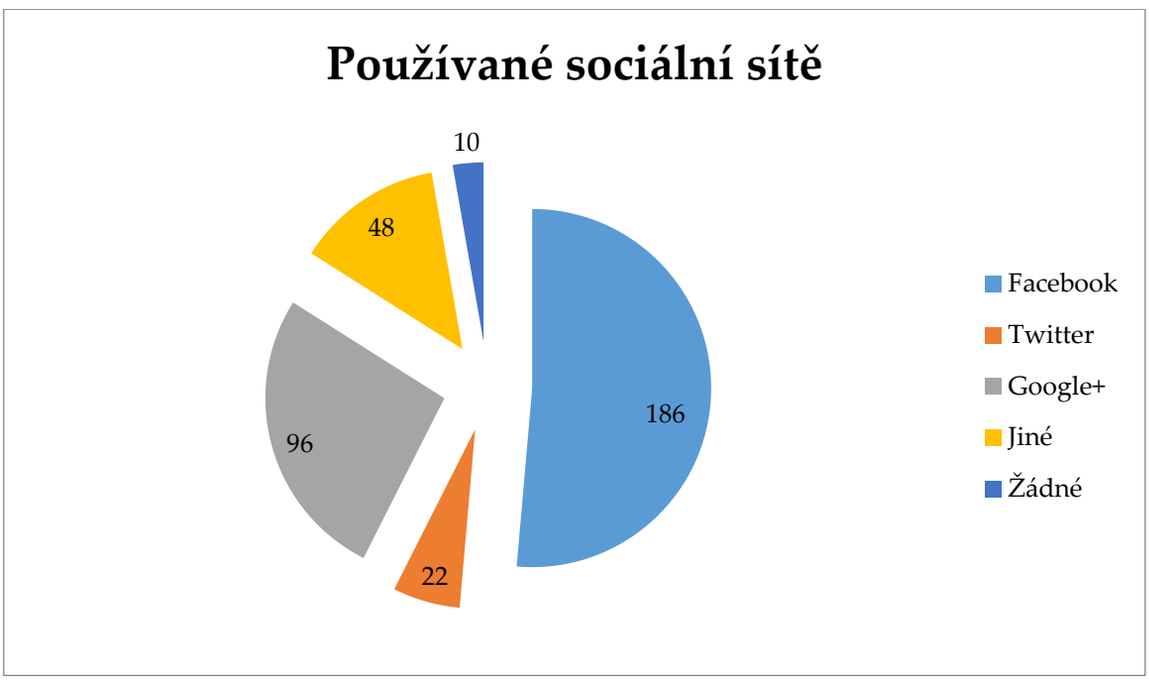
Schopnost ovládání PC	počet respondentů	podíl v %
Začátečník (ovládám kancelářské programy, procházení internetu)	46	23 %
Mírně pokročilý (instalace programů)	64	32 %
Pokročilý (nastavování aplikací, jednoduché administrátorské úkoly)	74	37 %
Profesionál (práce v příkazovém řádku, programování)	16	8 %
Celkem	200	100 %

V této otázce měli respondenti zhodnotit, za jak schopné uživatele počítačů se považují. Příjemné zjištění je, že 77 % respondentů se považuje za alespoň mírně pokročilé uživatele PC a lepší, tedy by jim měla být známa rizika spojená s užíváním počítače připojeného do kyberprostoru. Celých 23 % respondentů se však považuje za začátečníky. Ti budou zřejmě nástrahami kyberprostoru ohroženi podstatně více.

Otázka č. 6 - Používáte některé ze sociálních sítí? (prosím zaškrtněte všechny Vámi používané)

- Facebook
- Twitter
- Google+
- Jiné
- Žádné

Graf 6 - Používané sociální sítě



Tabulka 6 - Používané sociální sítě

Užívané sociální sítě	četnost užívání sociální sítě	podíl v %
Facebook	186	93 %
Twitter	22	11 %
Google+	96	48 %
Jiné	48	24 %
Žádné	10	5 %

S ohledem na formu šíření dotazníku, jež byla zvolena a vzhledem ke stále se šířící oblibě sociálních sítí není překvapením, že pouze 5 % respondentů, nevyužívá žádné sociální sítě. Dotazník prokázal, že jednoznačně nejhojněji používanou sociální sítí u nás je určitě Facebook, který používá 93 % respondentů. S nadsázkou by se dalo říci, kdo není na Facebooku, jako by nebyl.

Otázka č. 7 - Víte co to je sociální inženýrství?

- Neslyšel jsem tento pojem.
- Pojem jsem slyšel, ale nevím, co znamená.
- Ano, vím, co pojem znamená.
- Ano, setkal jsem se osobně se sociálním inženýrstvím.

Graf 7 - Víte co to je sociální inženýrství

Tabulka 7 - Víte co to je sociální inženýrství

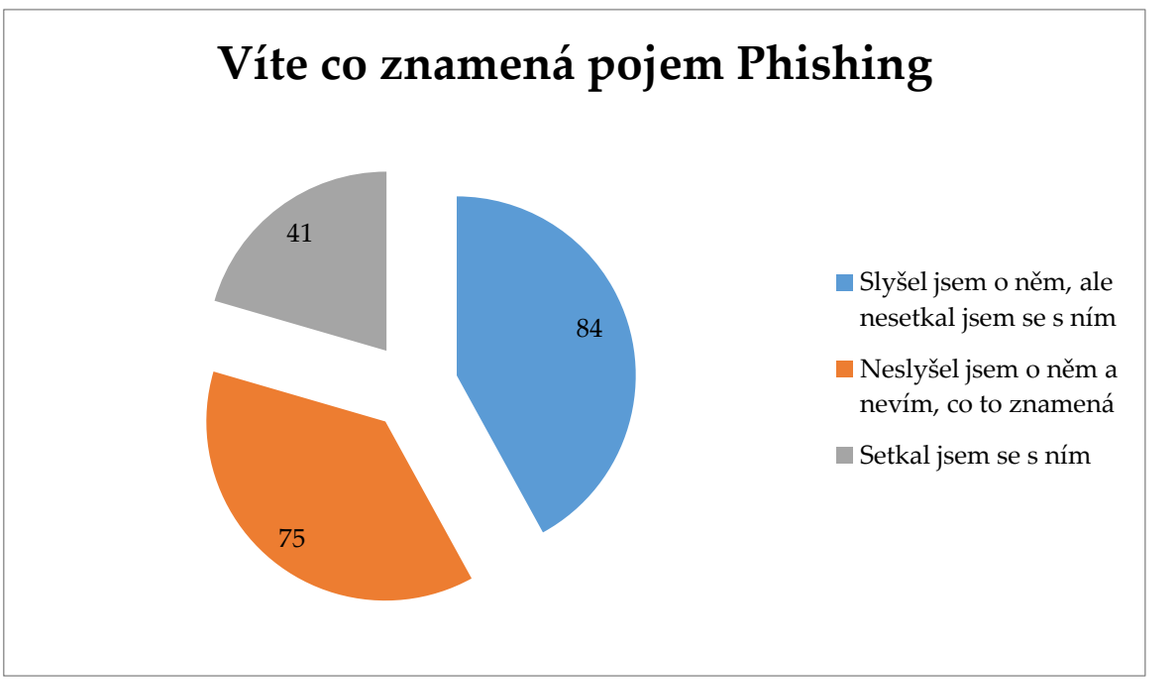
Co je sociální inženýrství	počet respondentů	podíl v %
Neslyšel jsem tento pojem	74	37 %
Pojem jsem slyšel, ale nevím, co znamená	62	31 %
Ano, vím, co pojem znamená	55	27,5 %
Ano, setkal jsem se osobně se sociálním inženýrstvím	9	4,5 %
Celkem	200	100 %

Pojem sociální inženýrství u nás není příliš známý. V médiích se o tomto problému u nás téměř nemluví na rozdíl od zahraničí. To je důvod, proč 68 % respondentů uvedlo, že pojem buď neslyšeli, nebo neví, co znamená. Pouze necelých 5 % respondentů ví o tom, že se stali terčem sociálního inženýrství. I když je jisté, že s nějakou formou sociálního inženýrství se setkalo mnohem více lidí.

Otázka č. 8 - Víte co znamená pojem Phishing a setkali jste se s ním?

- Slyšel jsem o něm, ale nesetkal jsem se s ním
- Neslyšel jsem o něm a nevím, co to znamená
- Setkal jsem se s ním

Graf 8 - Znalost pojmu phishing



Tabulka 8 - Znalost pojmu phishing

Znalost pojmu phishing	počet respondentů	podíl v %
Slyšel jsem o něm, ale nesetkal jsem se s ním	84	42 %
Neslyšel jsem o něm a nevím, co to znamená	75	37,5 %
Setkal jsem se s ním	41	20,5 %
Celkem	200	100 %

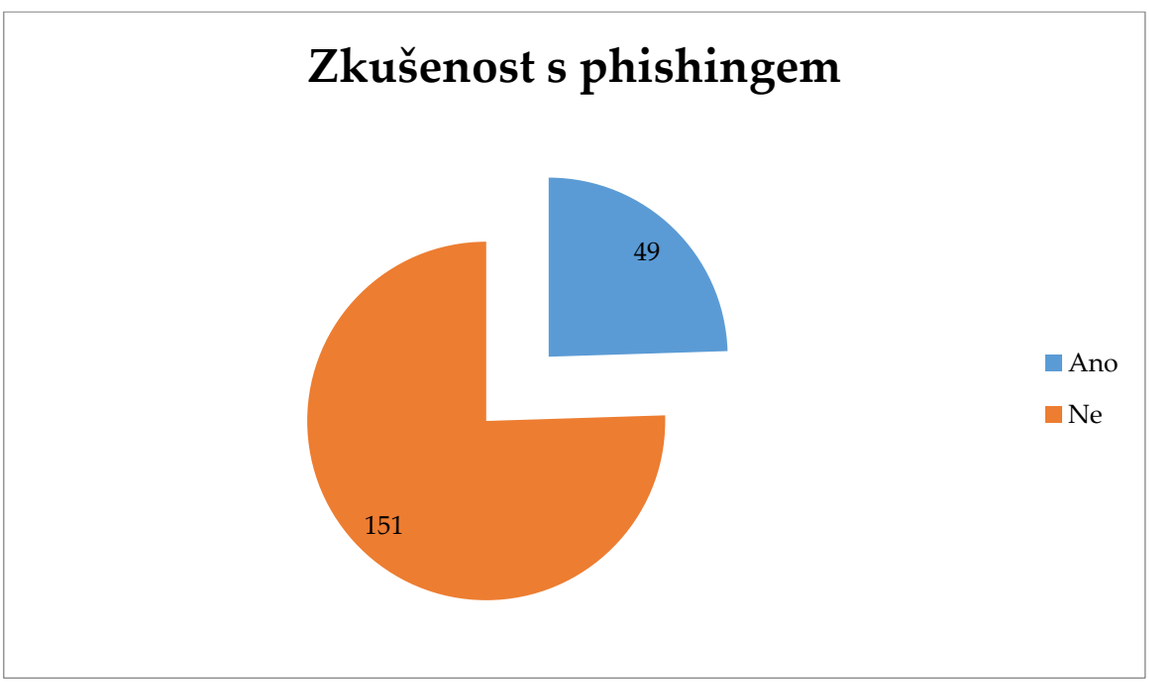
Phishing je jednou forem sociálního inženýrství, ale toto si uvědomuje málokdo. Z odpovědí na tuto otázku plyne, že minimálně s touto formou sociálního inženýrství se setkalo více než 20 % respondentů. Je alarmující, že tento pojem nezná více než 37 %

respondentů, přestože tato forma sociálního inženýrství je relativně často medializována. Zprávy o něm se objevují ve vlnách, vždy když se začne ve výraznější míře šířit nějaká zpráva tohoto typu.

Otázka č. 9 - Stalo se Vám, že Vám přišel email z banky nebo od provozovatele Vaší mailové schránky a žádal Vás o přihlášení?

- Ano
- Ne

Graf 9 - Zkušenost s phishingem



Tabulka 9 - Zkušenost s phishingem

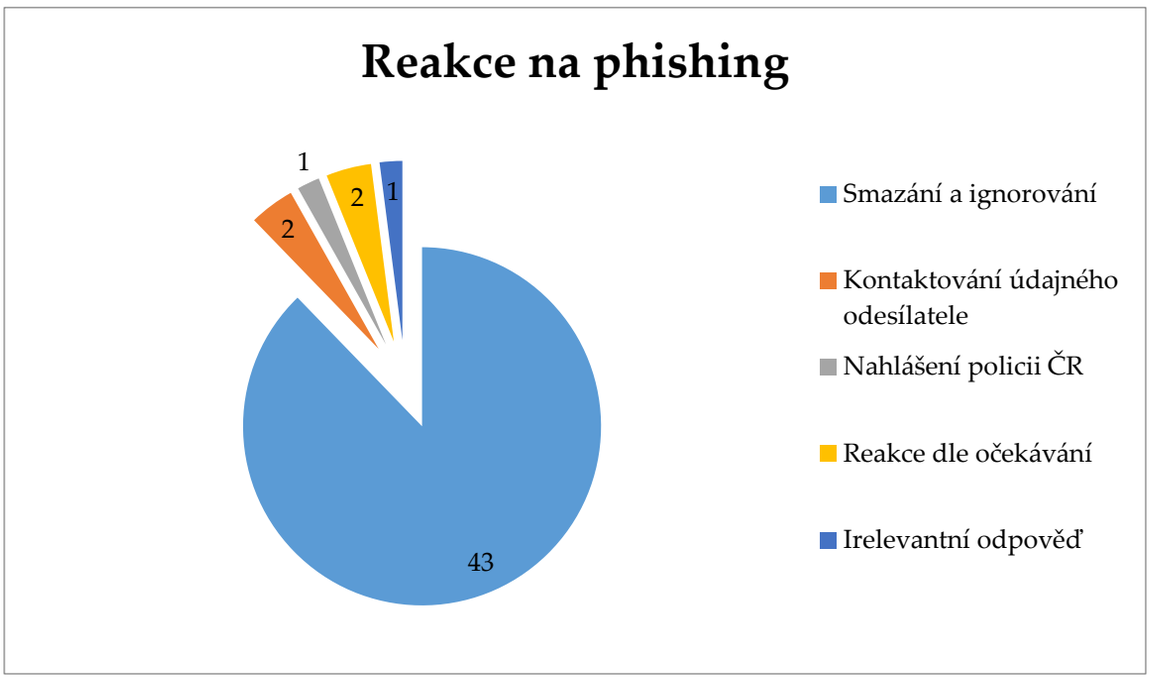
Zkušenost s phishingem	počet respondentů	podíl v %
Ano	49	24,5 %
Ne	151	75,5 %
Celkem	200	100 %

Je zajímavé, že v předchozí otázce přiznalo pouze 20,5 % respondentů, že se setkali s phishingem. V této otázce toto potvrdilo téměř 25 % dotázaných. Zřejmě ona 4 % rozdílu patří do kategorie „nevím, co to znamená“, ale pokud je jim předložen konkrétní případ, vzpomenou si, že už se jim něco takového stalo.

Otázka č. 10 - Jaká byla Vaše reakce na tento email?

Jedná se o otevřenou otázku, která byla přístupná pouze části respondentů, kteří na předchozí otázku odpověděli ano. Pozitivní je, že z respondentů, kteří se stali potencionální obětí phishingu, reagovala dle požadavků útočníka pouhá 4%, dále již nebylo zjišťováno, jaké dopady to na tyto respondenty mělo. Bohužel se vyskytla jedna irelevantní odpověď, která neměla s otázkou vůbec nic společného, to jsou 2 % odpovědí. Zbylých 94 % respondentů reagovalo správně, ze 46 odpovědí byly pouze 3 reakce, které se odlišovaly od zbytku správných odpovědí. V jednom případě respondent kontaktoval policii ČR, což je správná reakce, ale nebylo dále zjišťováno, s jakým úspěchem se policie s tímto případem vypořádala. Vzhledem k tomu, že při takovýchto útocích bývá použito botnetu, případně anonymizovaná IP adresa útočníka, je pravděpodobnost odhalení pachatele minimální. V dalších 2 případech cíle útoku kontaktovaly údajného odesílatele phishingu a dále tento útok řešily ve spolupráci s údajným odesílatelem. Zbylých 43 respondentů reagovalo odstraněním inkriminovaného e-mailu bez jakékoliv reakce na něj.

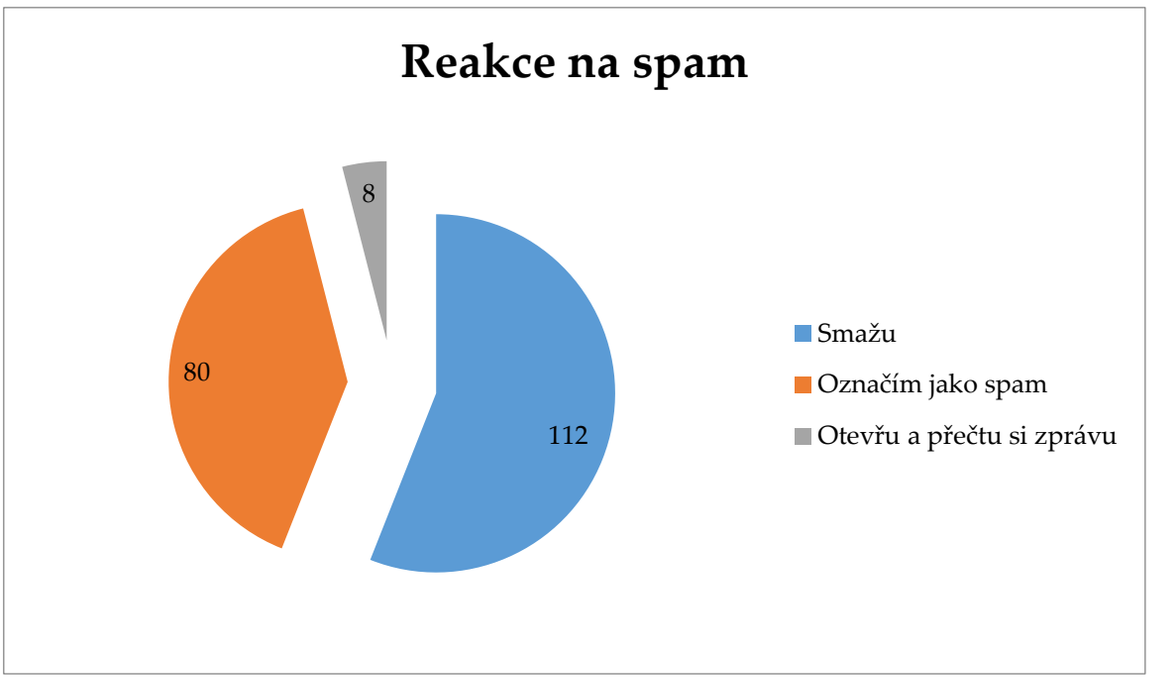
Graf 10 - Reakce na phishing



Otázka č. 11 - Jaká je Vaše reakce na neznámý email zcela zřejmě reklamního charakteru?

- Smažu
- Označím jako spam
- Otevřu a přečtu si zprávu

Graf 11 - Reakce na spam



Tabulka 10 - Reakce na spam

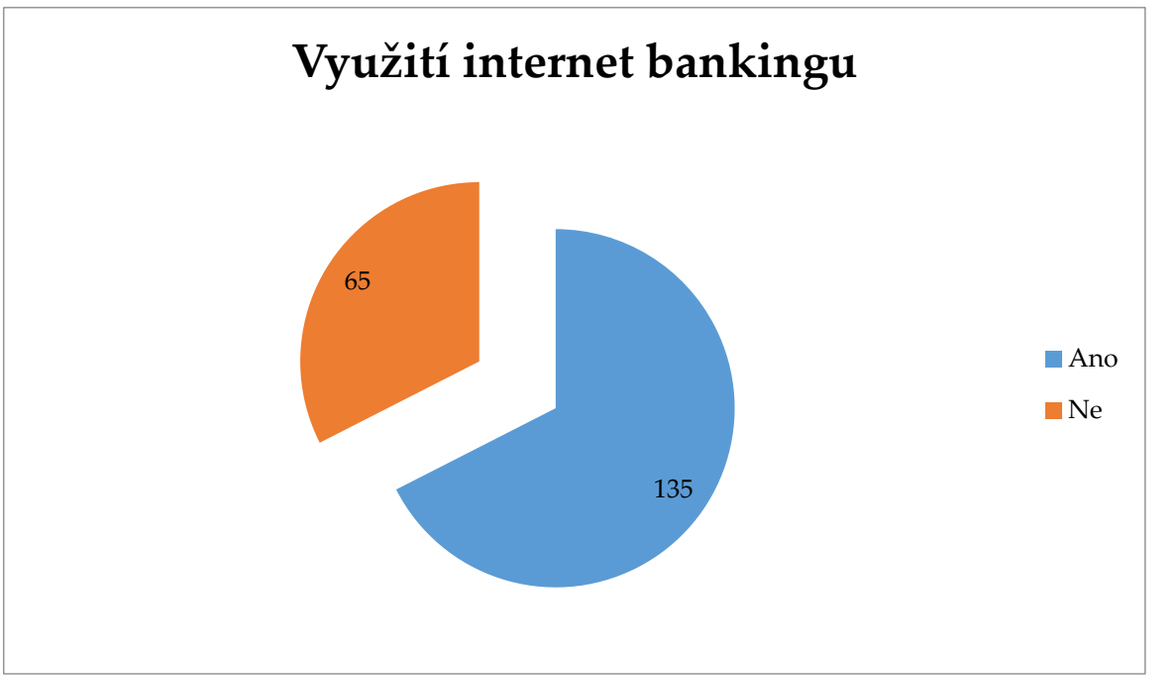
Reakce na spam	počet respondentů	podíl v %
Smažu	112	56 %
Označím jako spam	80	40 %
Otevřu a přečtu si zprávu	8	4 %
Celkem	200	100 %

Spam není až tak velkým nebezpečím jako spíše obtěžující věcí, ale podle reakcí respondentů pouze 4 % z nich se spamovými zprávami zabývají. Zbylých 96 % spamovou zprávu buď smaže, nebo označí jako spam pro spam filtr a následně odstraní.

Otázka č. 12 - Využíváte internet banking (případně bankovní aplikaci ve smartphonu)?

- Ano
- Ne

Graf 12 - Využití internet bankingu



Tabulka 11 - Využití internet bankingu

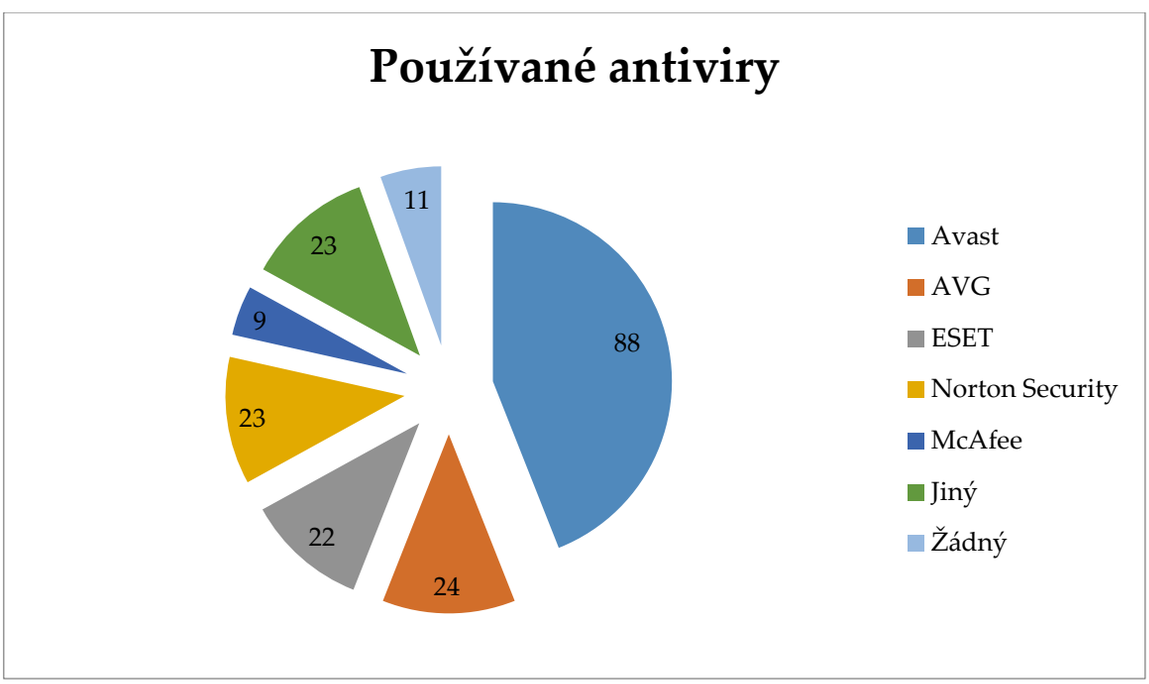
Využití internet bankingu	počet respondentů	podíl v %
Ano	135	67,5 %
Ne	65	32,5 %
Celkem	200	100 %

Více než 2/3 respondentů využívá internet banking nebo online aplikaci v mobilním telefonu, což svědčí o důvěře respondentů v tyto nástroje přímého bankovnictví, ale je třeba počítat s tím, že tato forma obsluhy účtu sebou přináší i svá rizika.

Otázka č. 13 - Jaký používáte antivirový program v PC?

- Avast
- AVG
- ESET
- Norton Security
- McAfee
- Jiný
- Žádný

Graf 13 - Používané antiviry



Tabulka 12 - Používané antiviry

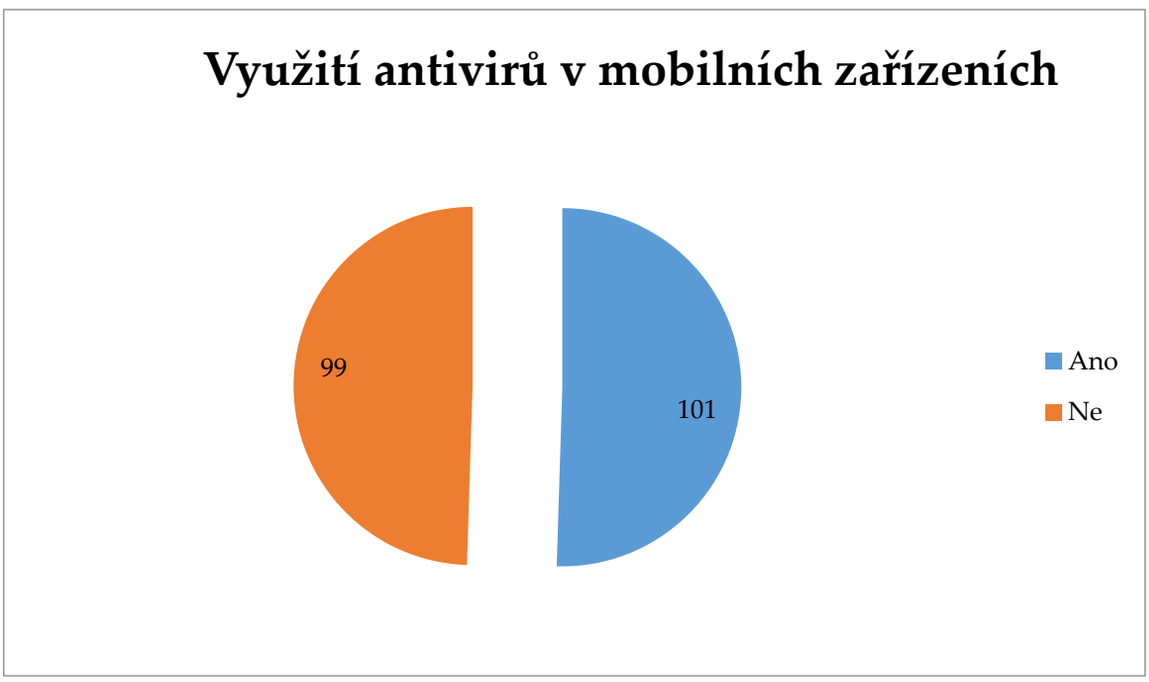
Vyžívané antiviry	počet respondentů	podíl v %
Avast	88	44 %
AVG	24	12 %
ESET	22	11 %
Norton Security	23	11,5 %
McAfee	9	4,5 %
Jiný	23	11,5 %
Žádný	11	5,5 %
Celkem	200	100,0 %

Jak vyplývá z odpovědí respondentů, nejrozšířenějším antivirovým programem v dotazované skupině je jednoznačně antivirový program firmy Avast. Jedná se o spolehlivý program, který je v základní verzi možno používat zdarma, pouze za zaregistrování tohoto programu. Tato verze zdarma ale neobsahuje prémiové funkce, které pomáhají počítač chránit i před dalšími hrozbami, než jsou pouze viry. Další 3 příčky téměř se shodnými výsledky (dohromady necelá 1/3 respondentů využívá některý z nich) obsadily AVG, ESET a Norton. Jedná se také o spolehlivé programy zajišťující v základu antivirový program zdarma, přičemž AVG je českého původu. Přesto se největší oblibě těší právě Avast.

Otázka č. 14 - Používáte nějaký antivirový program ve smartphonu nebo tabletu?

- Ano
- Ne

Graf 14 - Využití antivirů v mobilních zařízeních



Tabulka 13 - Využití antivirů v mobilních zařízeních

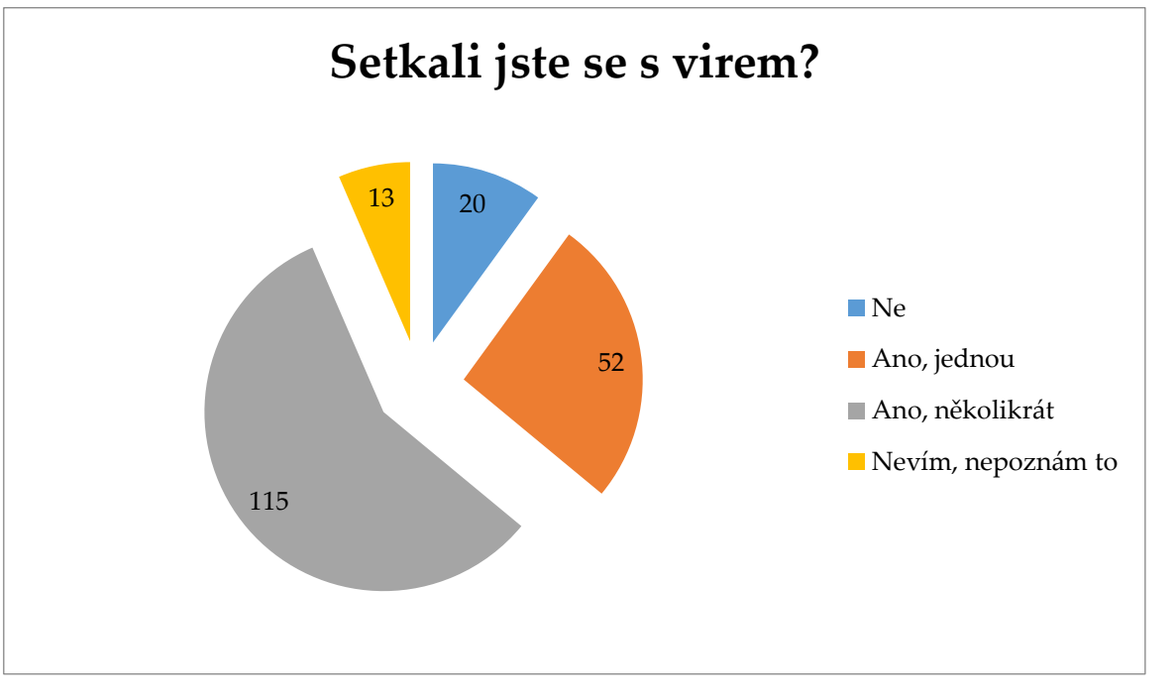
Využití antivirů v mobilních zařízeních	počet respondentů	podíl v %
Ano	101	50,5 %
Ne	99	49,5 %
Celkem	200	100,0 %

Dalším příjemným zjištěním je, že plná polovina respondentů nepodceňuje nebezpečí virů ani u mobilních zařízení. Doby, kdy mobilní telefon byl jen telefon, jsou již dávno pryč. V současné době je většina mobilních telefonů dosti výkonnými počítači s operačním systém, který může být napaden virem. Proto je vhodné i mobilní telefon, potažmo tablet, chránit antivirovým programem stejně jako počítač.

Otázka č. 15 - Setkali jste se ve svém počítači s virem?

- Ne
- Ano, jednou
- Ano, několikrát
- Nevím, nepoznám to

Graf 15 - Setkali jste se s virem



Tabulka 14 – Setkali jste se s virem

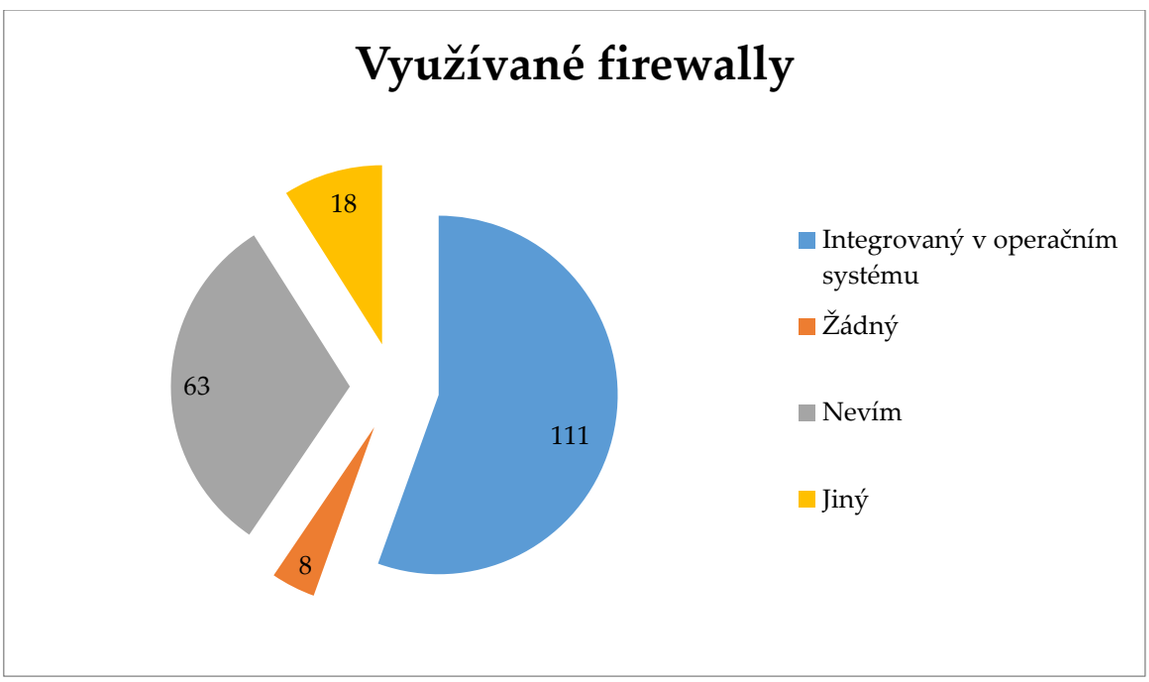
Setkání se s virem	počet respondentů	podíl v %
Ne	20	10 %
Ano, jednou	52	26 %
Ano, několikrát	115	57,5 %
Nevím, nepoznám to	13	6,5 %
Celkem	200	100,0 %

Není překvapením, že více než 75 % respondentů se setkalo s virem. Otázkou je, jak velká část respondentů považovala za viry další škodlivý software, jako jsou červi a trojští koně. Tyto škodliviny označují antivirové programy také jako viry.

Otázka č. 16 - Jaký používáte Firewall?

- Integrovaný v operačním systému
- Žádný
- Nevím
- Jiný

Graf 16 - Využívané firewally



Tabulka 15 - Využívané firewally

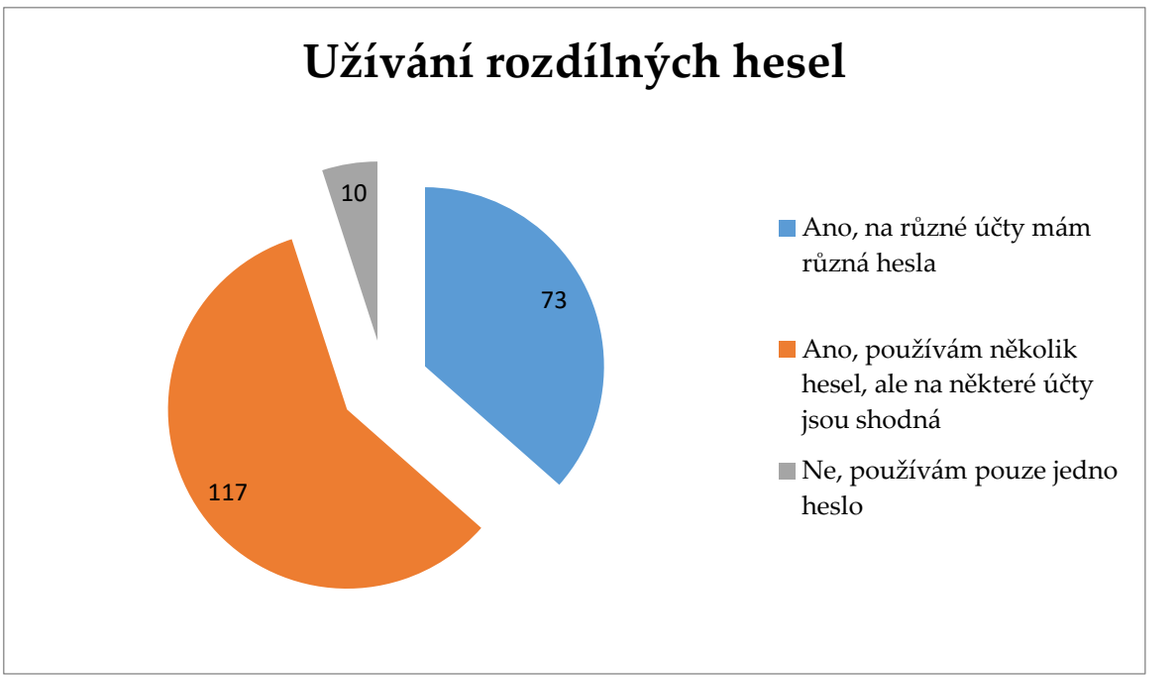
Využívané firewally	počet respondentů	podíl v %
Integrovaný v operačním systému	111	55,5 %
Žádný	8	4 %
Nevím	63	31,5 %
Jiný	18	9 %
Celkem	200	100 %

Vzhledem k tomu, že drtivá většina uživatelů PC používá operační systém Microsoft Windows, který má implementovaný firewall, je velice pravděpodobné, že ti respondenti, kteří odpověděli „nepoužívám žádný firewall“, využívají právě tento implementovaný, aniž by o tom věděli. Stejně tak i respondenti, odpovídající „nevím“, s největší pravděpodobností používají také tento implementovaný. Pouze 9 % respondentů uvedlo „jiný“, tito mají zřejmě skutečné povědomí o tom, co firewall je a k čemu slouží.

Otázka č. 17 - Používáte různá hesla nebo jen jedno univerzálně všude?

- Ano, na různé účty mám různá hesla.
- Ano, používám několik hesel, ale na některé účty jsou shodná.
- Ne, používám pouze jedno heslo.

Graf 17 - Užívání rozdílných hesel



Tabulka 16 - Užívání rozdílných hesel

Užívání rozdílných hesel	počet respondentů	podíl v %
Ano, na různé účty mám různá hesla.	73	36,5 %
Ano, používám několik hesel, ale na některé účty jsou shodná.	117	58,5 %
Ne, používám pouze jedno heslo.	10	5 %
Celkem	200	100 %

Používat různá hesla na různé stránky doporučuje většina expertů na IT bezpečnost. Je to z toho důvodu, že pokud se útočníkovi podaří prolomit přístup na účast na nějaké službě, může zkusit použít stejné údaje i na přihlášení na jinou službu. Jak ukazuje nejpoužívanější odpověď, téměř 60 % respondentů používá několik různých hesel, což není zcela nejbezpečnější. Přesto je to určitě bezpečnější, než jak uvádí 5 % respondentů používat pouze jedno heslo. Nejbezpečnější z pohledu expertů by bylo mít na každé službě, na každém serveru, na každém účtu jiné heslo. Toto má pouze jeden limit, a tím

je lidská paměť. Pokud budeme brát ideální heslo, které by mělo mít 8- 10 znaků, mělo by obsahovat číslice, malá písmena, velká písmena a případně speciální znaky a na druhou stranu by nemělo obsahovat celá slova. To by si člověk nemohl pamatovat téměř nic jiného, než kombinace souvisejících přihlašovacích údajů a hesel společně s účtem, ke kterému daná kombinace patří.

3.4 Vyhodnocení hypotéz a komparace výsledků

V této části bakalářské práce se nachází vyhodnocení stanovených hypotéz a komparace výsledků provedeného průzkumu s jinou prací podobně tematicky zaměřenou. Pro komparaci byla zvolena bakalářská práce na téma: Bezpečnost na internetu (Šimoník, 2013). Pod vyhodnocením jednotlivých hypotéz bude následně porovnání výsledků získaných šetřením uvedených v předchozí kapitole s výsledky získanými Šimoníkem v roce 2013 na podobné otázky. Zaměříme se zejména na otázky spojené s výše stanovenými hypotézami.

Hypotéza 1 - Předpokládáme, že více než 70 % respondentů používá minimálně jednu sociální síť.

K hypotéze 1 se vztahovala otázka č. 6. U této otázky bylo možné označit více odpovědí, aby bylo zřejmé, které sociální sítě jsou mezi respondenty využívány. Výsledkem je, že pouhých 5 % respondentů nepoužívá žádnou sociální síť. Na druhou stranu 93 % respondentů využívá zřejmě nejrozšířenější a u nás určitě nejznámější sociální síť Facebook. Světově obrovské množství uživatelů této sítě je důvodem, že se na ni čím dál více zaměřují různí kyberzločinci a snaží se zde buď šířit různý škodlivý software, jako jsou trojští koně a červi, nebo po zcizení uživatelského účtu vylákat od nic netušících kontaktů, uvedených v přátelích, drobné finanční částky. Pokud se oběť nechá přesvědčit k zaslání jakékoli, dalo by se říci téměř bezvýznamné částky (řádově se běžně

v takovýchto případech jedná o desítky korun), potom se většina uživatelů takto nízkou částkou nebude vůbec zabývat a odepíše ji. A to je to na co útočník spoléhá, že nikdo nebude pátrat po takto nízké částce, ale zároveň spoléhá i na to, že bude reagovat dostatečně mnoho přátel majitele napadeného účtu, kteří peníze pošlou.

Na druhém místě oblíbenosti se u respondentů umístila síť, kterou provozuje firma Google s označením Google+. Uživatelem této sítě se stává automaticky každý, kdo si na stránkách firmy Google založí účet.

Pouhých 11 % respondentů uvedlo používání ve světě a hlavně v USA velice oblíbenou síť Twitter.

Hypotéza číslo 1 byla POTVRZENA

Výsledek získaný tímto průzkumem koresponduje s výsledkem získaným Šimonikem (2013). V jeho případě byla četnost využívání Facebooku na „pouhých„56 %. I přestože někteří lidé upouštějí od používání sociálních sítí, je více než pravděpodobné, že sociální sítě budou součástí našich životů ještě po dlouhou dobu. Vzhledem ke kvantitě jejich využívání, je velice pravděpodobné, že se budou ještě více potýkat s problémy, které se zde objevují i nyní (malware, sociální inženýrství).

Hypotéza 2 - Předpokládáme, že více než 50 % respondentů ví, co znamená pojem sociální inženýrství.

K hypotéze 2 se vztahovala otázka č. 7. Zde jsme se dotazovali, zda respondenti znají pojem sociální inženýrství a výsledek je dosti neuspokojující. Celých 68 % respondentů, buď vůbec netuší o tom, že něco jako sociální inženýrství existuje, nebo se s pojmem

setkali, ale netuší, co znamená. Tato čísla jsou znepokojující. Zbývajících 32 % ví, co pojem znamená a pouhá 4 % respondentů ví, že se se sociálním inženýrstvím setkala. Vzhledem k nedostatečné povědomosti o této hrozbě, není toto zjištění příliš vypovídající, protože nemůžeme posoudit, kolik respondentů z oněch 68 %, kteří nevědí, co sociální inženýrství je, bylo tomuto útoku vystaveno, aniž by o tom věděli.

Hypotéza číslo 2 byla VYVRÁCENA

S ohledem na důvěřivost českého národa můžeme být rádi, že se zde zatím neobjevil tak schopný sociotechnik, jakým je K. Mittnick. Je více než alarmující, že 68 % respondentů neví, co se pod pojmem sociální inženýrství skrývá. Šimonik (2013) dospěl k podobným výsledkům. V jeho případě, ale pouhých 22 % dotázaných vědělo, co se za pojmem skrývá. V našem případě to bylo 31 %, z toho 4 % se dokonce s praktikami sociálního inženýrství setkalo osobně. Toto je zřejmě nejvíce alarmující zjištění tohoto výzkumu a je to oblast, kde by se měla zjednat náprava. Je možné zlepšit informovanost o tomto problému mezi současnou mladou generací, která ještě navštěvuje nějaký stupeň vzdělání v rámci výuky předmětu IT. Pro dospělou populaci by bylo potřeba toto téma více medializovat. Média by se mohla věnovat více takovýmto kauzám. Je velice pravděpodobné, a pokud se podíváme na výsledky prezentované Šimonikem (2013), tak zřejmě téměř nikdo u nás nebude znát jméno, Kevin Mittnick, který se stal v USA hvězdou číslo 1, i když zřejmě nechtěně. Jeho kauzy byly v USA značně medializovány a z tohoto důvodu je tam mnohonásobně větší povědomí o sociálním inženýrství. Toto je část kyberbezpečnosti, které by mělo být věnováno mnohem více pozornosti.

Hypotéza 3 - Předpokládáme, že více než 50 % respondentů se setkalo s phishingem.

K hypotéze 3 se vztahovaly otázky č. 8-10. V těchto otázkách jsme se dotazovali na povědomost o pojmu phishing, na setkání se s phishingem a případnou reakci na něj. V otázce povědomosti o phishingu téměř 62 % respondentů uvedlo, že vědí, co je phishing a pouhých 19 % se s ním setkalo.

Toto zcela nekoresponduje s následující otázkou, která zjišťovala, kolik respondentů se setkalo s něčím, co se dá označit za phishing. Zde uvedlo, že se s podobným útokem setkalo dokonce 24 % respondentů. Je tedy otázkou, jestli oněch 5 % rozdílu je z těch 38 % respondentů, kteří uvedli, že nevědí co phishing je, nebo zda spadají do skupiny, která uvedla, že ví co je phishing, ale ve skutečnosti to nevěděli a s phishingovým útokem se setkali.

Poslední z těchto otázek se věnovala reakci na phishingový útok. Tato otázka byla přístupná pouze respondentům, kteří na otázku č. 9 odpověděli „ano“. Jednalo se o otevřenou otázku, kde respondenti odpovídali, jak reagovali na zprávu, která zřejmě byla phishingovým útokem. Zde byla získána jedna zcela nerelevantní odpověď. Ostatní odpovědi byly relevantní. Jak je vidět z odpovědí, téměř všichni, kdo měli aktivní zkušenost s phishingem zareagovali tak, jak měli, a tj., buď zprávu ignorovali, smazali, nebo zablokovali. Je zde několik výjimek, které nezapadají ani do jedné z předchozích 3 kategorií. 3 jsou správné, a to ve dvou případech odpověděli respondenti, že si ověřili pravost doručené zprávy a reagovali podle doporučení údajného odesílatele, a ne podle očekávání útočníka. Další výjimečnou, ale také správnou odpovědí je nahlášení na PČR. Je pravděpodobné, že policie nemá dostatečné kapacity na řešení každého phishingového útoku. Vzhledem k existenci botnetů je velice nepravděpodobné, že odhalení skutečného útočníka je vůbec možné. Dvě odpovědi jsou absolutně špatně.

Jsou to odpovědi, kdy respondenti reagovali podle očekávání útočníka a tato akce mohla mít pro ně velice nepříjemné důsledky.

Hypotéza číslo 3 byla VYVRÁCENA

Uklidňujícím pro nás může být fakt, že díky médiím a jejich informování o podobných případech, téměř všichni respondenti reagovali zcela adekvátně a pouze dva respondenti se nechali útočníkem oklamat a reagovali podle jeho očekávání. Pro nás by bylo zajímavé, jaké následky tyto zřejmě zdařilé útoky měly pro naše respondenty, ale toto nebylo součástí šetření a není možné již zjistit, kteří respondenti takto odpověděli. Dá se považovat za velký pokrok oproti Šimonikovi (2013) počet respondentů, kteří zřejmě vědí, co je phishing, neboť v jeho průzkumu se uvádí, že pouhých 13 % respondentů vědělo, co phishing je a pouhá 3 % z nich se s ním setkala. Toto považujeme relativně za velký pokrok, protože v našem případě o phishingu mělo alespoň tušení, co by to mohlo být, necelých 62 % respondentů, což je téměř 5x více než v případě Šimonika (2013). Tento nárůst je zřejmě spojen s medializací několika případů phishingových útoků. Hlavně byly medializovány pokusy o získání přístupových jmen a hesel klientů významných českých bank.

Hypotéza 4 - Předpokládáme, že více než 75 % respondentů používá antivirový program.

K hypotéze 4 se vztahovala otázka č. 13. V této otázce bylo zjišťováno, jaké antivirové programy respondenti používají. Pouze 5,5 % respondentů uvedlo, že nepoužívá žádný antivirový program, což je potěšující zpráva. Jako možnosti byly zvoleny zřejmě nejrozšířenější antivirové programy u nás. Není překvapením, že nejpoužívanějším se stal antivirový program Avast, který je pro soukromé použití v domácnosti distribuován zdarma, pouze za zaregistrování. Tento antivirový program využívalo téměř 44 %

respondentů. Dalších 38 % zbylo na další 4 významné hráče na trhu. Nebudeme řešit, zda jsou lepší nebo horší než Avast. Zdarma jsou jen verze, které obsahují samostatný antivirový software. Další doplňkové funkce jsou pouze v placených verzích těchto programů.

Hypotéza číslo 4 byla POTVRZENA

Vzhledem k tomu, že antivirový program je základní ochranou každého počítače, není nijak překvapující, že dle odpovědí respondentů v tomto průzkumu nepoužívá žádný antivirový program 5,5 % respondentů. Šimoník (2013) získal velice podobný výsledek. V jeho případě nepoužívalo žádný antivirový program 6 % respondentů. Rozdíl 0,5 % se dá považovat za zanedbatelný s ohledem na relativně nízké počty respondentů. I ohledně používaných antivirových programů byly získány velice podobné údaje jako v případě Šimoníka (2013). Avast v průzkumu pro tuto práci získal 44 % respondentů, v případě Šimoníka (2013) 45 %. AVG 11 % ku 12 % a ostatní antivirové programy získaly více rozdílné sympatie respondentů, ale toto již není tak podstatné. Nejpodstatnější je otázka nepoužívání antiviru a ta dopadla nad očekávání dobře.

Hypotéza 5 - Předpokládáme, že více než 70 % respondentů se setkalo ve svém počítači s počítačovým virem.

K hypotéze 5 se vztahuje otázka č. 15. V této otázce jsme se dotazovali, zda se respondenti setkali ve svém PC s virem. Téměř 84 % respondentů se s virem ve svém PC setkalo nejméně jednou. Celých 57 % respondentů se setkalo s virem několikrát. Další otázkou je, kolik z těchto napadení PC byly skutečně viry a v kolika případech se jednalo o jiný škodlivý software (trojské koně, nebo červy). Ale toto by nám dokázal zodpovědět málokdo z dotazovaných, z toho důvodu, že všechny tyto útoky dokáží

vyhodnotit antivirové programy, a tak je pravděpodobné, že vše co označil antivirový program za hrozbu, by respondenti označili za virus. Tedy bychom hypotézu považovali za potvrzenou.

Hypotéza číslo 5 byla POTVRZENA

Zde byl očekáván velký podíl respondentů, kteří se setkali s virem či jiným malwarem, který antivirové programy označí jako vir, neboť současný internet a e-mailová komunikace je viry, trojskými koni a červy, velmi bohatě zásobena. Čas od připojení PC k internetu do prvního pokusu o jeho napadení se v roce 2004, podle studie Internet Storm Center při SANS Institutu, pohyboval průměrně kolem 20 minut. V současnosti je to řádově desítky sekund. V tomto výzkumu se s virem, ať už jednorázově, či opakovaně setkalo přes 83 %, v případě Šimonika (2013) to bylo 69 %. Nelze jednoznačně říci, že by se jednalo o nějak významný nárůst. Tento nárůst bude velice ovlivněn pouze zkušenostmi velmi omezeného vzorku respondentů.(ŠIMONÍK, 2013)

Z výzkumu vyplývá, že průzkumný vzorek respondentů využíval vzhledem k odpovědi na otázku č. 4. kyberprostor velmi často (alespoň hodinu denně využívalo internet 98 % respondentů). S ohledem na toto by měla být informovanost o hrozbách kyberprostoru výrazně vyšší. V případě většiny otázek dopadly výsledky nad očekávání dobře, ale v otázce informovanosti o sociálním inženýrství dopadly výsledky dosti nelichotivě. Vzhledem k tomu, že se jedná o velice výraznou hrozbu, by bylo potřeba více informovat veřejnost o těchto hrozbách. Jednou z možností by byla výraznější medializace odhalených případů sociotechniků, jako tomu bylo např. v USA s kauzou Kevina Mitnicka.

ZÁVĚR

Hlavním cílem práce bylo seznámení čtenářů s hlavními hrozbami kyberprostoru, které ohrožují běžné uživatele. Toto je rozvedeno v teoretické části práce, kde jsou popsány jednotlivé hrozby způsobem srozumitelným běžnému i začínajícímu uživateli kyberprostoru. Jsou zde nastíněny jednoduché způsoby ochrany a obrany počítače před hrozbami, kterým se dá bránit pomocí softwarových nebo hardwarových prostředků. Tyto možnosti by měly být naprostým základem toho, jak se bránit před kyberzločinem. Jednoduše řečeno, v každém počítači, který je připojen k internetu, by měl běžet minimálně antivirový program a alespoň základní firewall obsažený například v některých operačních systémech. Nejvíce jsou ohroženy počítače s operačním systémem Microsoft Windows. Počítače, na kterých běží zřejmě druhý nejrozšířenější operační systém Linux, nejsou tak častým cílem kyberzločinců. Jsou zde popsány také některé z mnoha jednoduchých, ale účinných metod a postupů sociálního inženýrství, na které by si měli uživatelé dávat pozor. Mimoto zde zmiňujeme některé nešvary uživatelů na sociálních sítích, kterým je dobré se vyvarovat.

V praktické části této práce jsme zjišťovali, na vzorku respondentů ve věku od 15 do 73 let, jak jsou na tom se znalostmi hrozeb, které na ně číhají v kyberprostoru. Zde jsme zjistili, že povědomí o většině hrozeb, na které jsme se ptali, respondenti celkově měli. Jen otázka směřující k sociálnímu inženýrství jako takovému nedopadla vůbec dobře. Je to dáno tím, že mnoho uživatelů se o hrozby nezajímá. Případy týkající se velké části ostatních hrozeb, jsou často medializovány. Pokud se takováto informace objeví několikrát v hlavních zprávách, je dost pravděpodobné, že si ji uživatelé zapamatují. U nás se zatím nevyskytlo mnoho případů sociálního inženýrství, proto nebyl tento problém tolik medializován. Abychom byli přesní, jedna z forem se u nás vyskytuje relativně často a tou je phishing. A jak jsme zjistili ve

výzkumné části, ti kteří se s phishingem setkali, většinou zareagovali správně. Toto povědomí o phishingu bude dáno právě tím, že se u nás vyskytuje relativně. Opakují se vlny, kdy se začne nějaký phishingový útok vyskytovat ve větší míře a následně na toto zareagují média, nejčastěji ve zpravodajských relacích, a varují obyvatelstvo na co si dávat pozor.

Jak zvýšit informovanost obyvatelstva ohledně hrozeb vyjmenovaných v této práci? To je složitá otázka. Na nebezpečí na silnicích upozorňovala například reklamní kampaň ministerstva dopravy s názvem „Nemyslíš, zaplatíš!“, která odstrašujícím způsobem upozorňovala převážně řidiče, na nejčastější příčiny tragických nehod. Možná by nebylo od věci vymyslet a medializovat podobnou kampaň na téma hrozeb kyberprostoru. Zde je ale problém v tom, že v tomto případě nejde o životy ani o zdraví, ale „pouze“ o majetek, tak proč by do tohoto tématu měly být investovány prostředky. Další možností, jak již bylo zmíněno výše, je věnovat těmto hrozbám více prostoru při hodinách výpočetní techniky na všech stupních vzdělávání. Jednou z nejvíce ohrožených skupin jsou aktivní senioři. Pro které by byly vhodné kurzy a besedy věnující se této problematice. V současné době jedinou možností, jak se o těchto hrozbách dozvědět více, je sebevzdělávání. Každý, kdo se posadí k počítači, který je připojený do internetu, má možnost snadno tuto problematiku dohledat.

Kyberprostor je nebezpečná část světa, kde na každého číhá mnoho hrozeb. Pokud se jim budeme chtít úspěšně vyvarovat, bude muset každý z nás věnovat nějaký čas svému vzdělávání se. Pokud tomu tak nebude, velice snadno se staneme obětí kyberzločinu.

4 SEZNAM POUŽITÉ LITERATURY

BEDNÁŘ, Vojtěch. Pharming je zpět a silnější. 2007. *Lupa.cz.* [Online] 23. 3 2007. [Citace: 29. 3 2016.] http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/.

BITTO, Ondřej. *Jak zabezpečit domácí malou síť Windows XP.* 2006. Brno : Computer Press, 2006. ISBN 8025110982.

BITTO, Ondřej. Rhybaření střídá pharming. 2005. *Lupa.cz.* [Online] 31. 3 2005. [Citace: 29. 3 2016.] http://www.lupa.cz/clanky/rhybareni-strida-pharming/.

BITTO, Ondřej. Trojské koně: co jsou zač a jak se bránit - Živě.cz. 2005. *Živě.cz.* [Online] 30. 03 2005. [Citace: 25. 03 2016.] http://www.zive.cz/Clanky/Trojske-kone-co-jsou-zac-a-jak-se-branit/sc-3-a-123708/default.aspx.

CSIRT. CSIRT: Intrusion Detection Systém. 2015. *CSIRT.CZ.* [Online] 31. 08 2015. [Citace: 10. 03 2016.] https://www.csirt.cz/page/2963/intrusion-detection-system-a-csirt.cz/.

EINSTEIN, Albert. Pouze dvě věci jsou... *AZCITATY.CZ.* [Online] [Citace: 05. 03 2016.] http://azcitaty.cz/albert-einstein/14875/.

HÁK, Igor. Kniha.pdf. 2005. *Viry.cz.* [Online] 15. 09 2005. [Citace: 16. 03 2016.] http://viry.cz/download/kniha.pdf.

CHRISTENSEN, John. CNN - The trials of Kevin Mittnick - March 18, 1999. 1999. *http://edition.cnn.com/.* [Online] CNN, 18. 03 1999. [Citace: 31. 03 2016.] http://edition.cnn.com/SPECIALS/1999/mitnick.background/.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 2007. Praha : Grada, 2007. ISBN 9788024715612.

KASPERSKY LAB. Adware| Internet Security Threats| Kaspersky Lab. *Kaspersky Lab.* [Online] Kaspersky Lab. [Citace: 02. 04 2016.] http://www.kaspersky.com/cz/internet-security-center/threats/adware.

KASPERSKY LAB. Co je Warholův červ?| Warhol Worm Definition| Kaspersky Lab. *Kaspersky Lab.* [Online] Kaspersky Lab. [Citace: 31. 03 2016.] http://www.kaspersky.com/cz/internet-security-center/definitions/warhol-worm.

KASPERSKY LAB. Co je brána firewall?| Definice pojmu brána firewall| Kaspersky Lab. *Kaspersky Lab.* [Online] Kaspersky Lab. [Citace: 30. 03 2016.] http://www.kaspersky.com/cz/internet-security-center/definitions/firewall.

KASPERSKY LAB. Co je pharming?|Pharming definition| Kaspersky Lab. *Kaspersky Lab.* [Online] [Citace: 28. 03 2016.] http://www.kaspersky.com/cz/internet-security-center/definitions/pharming.

KOCMAN, Rostislav a LOHNISKÝ, Jakub. *Jak se bránit virům, spamu, dialerům a spyware.* 2005. Brno : CP Books, 2005. ISBN 8025107930.

KOHOUTEK, Rudolf. Slovník cizích slov: kyberprostor. *Slovník cizích slov abz.* 2008. [Online] 30. 3 2008. [Citace: 19. únor 2016.] http://slovnik-cizich-slov.abz.cz/web.php/slovo/kyberprostor.

KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač.* 2015. Praha : Grada Publishing, a.s., 2015. ISBN 9788024754536.

KUNEŠ, Jakub. Co je sociální inženýrství? - 1.díl|PC World.cz. 2012. *PC World.cz.* [Online] 02. 06 2012. [Citace: 08. 03 2016.] http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-1-dil-44361.

MAYER, Marco, a další. Academia: How would you define Cyberspace? 2014. *Academia.* [Online] 19. 05 2014. [Citace: 01. 03 2016.] https://www.academia.edu/7096442/How_would_you_define_Cyberspace.

MICROSOFT. Spyware: What Is It and How to Prevent It. *www.microsoft.com.* [Online] Microsoft Corporation. [Citace: 01. 04 2016.] https://www.microsoft.com/en-us/safety/pc-security/spyware-whatis.aspx.

MIKLÁŠ, Michal. Informatika na gymnáziu jazykové škole s právem státní jazykové zkoušky Zlín. 2013. *www.gjszlin.cz.* [Online] 02. 09 2013. [Citace: 18. 03 2016.] http://www.gjszlin.cz/ivt/esf/ostatni-sin/pocitacove-viry.php.

MITNICK, Kevin D. a SIMON, William L. *Umění klamu.* 2003. Gliwice : Helion, 2003. ISBN 8373612106.

MITTELBACH, Jan. Pharming může ošálit i zkušenějšího uživatele internetu. 2008. *Hospodářské noviny.* [Online] 21. 3 2008. [Citace: 29. 3 2016.] http://tech.ihned.cz/c1-23480750-pharming-muze-osalit-i-zkusenejsiho-uzivatele-internetu.

PŘIBYL, Tomáš. Nebezpečí jménem phishing. 2007. *COMPUTERWORD.* [Online] 09. 01 2007. [Citace: 26. 03 2016.] http://computerworld.cz/securityworld/nebezpeci-jmenem-phishing-46139.

ROUSE, Margaret. What is social ingeneering? - definition of WhatIs.com. 2016. *WhatIs.com.* [Online] 02 2016. [Citace: 30. 03 2016.] http://searchsecurity.techtarget.com/definition/social-engineering.

ROUSE, Margaret. What is worm? - definition of WhatIs.com. 2016. *WhatIs.com.* [Online] 02 2016. [Citace: 30. 03 2016.] http://searchsecurity.techtarget.com/definition/worm.

STERLING, Bruce. Hacker_crackdown.pdf. *ZX magazín.* [Online] [Citace: 19. 02 2016.] http://zxm.speccy.cz/zxm/hacker_crackdown.pdf.

ŠIMONÍK, Petr. *Bezpečnost na Internetu.* 2013. Zlín : Univerzita Tomáše Bati ve Zlíně, 2013.

ŠTĚDROŇ, Bohumír a LUDVÍK, Miroslav. *Teorie bezpečnosti počítačových sítí.* 2008. Kralice na Hané : Computer Media, 2008. ISBN 9788086686356.

URBAN, Michal. Virii. *Gymnázium Beroun.* [Online] [Citace: 18. 03 2016.] http://www.gymberoun.cz/~hamernik/old/maturita/data/viry/viry.htm.

VÍTEK, Miloš a VÍTKOVÁ, Marcela. *Sociální vědy a inženýrství.* 2004. Hradec Králové : Gaudeamus, 2004. ISBN 807041474X.

5 SEZNAM POUŽITÝCH ZKRATEK

SCADA	Supervisory Control and Data Acquisition - Správa, řízení a sběr dat
CSIRT	Computer Security Incident Response Team – organizace zajišťující koordinaci řešení bezpečnostních hrozeb v počítačových sítích, které jsou provozovány na území ČR
NBÚ	Národní bezpečnostní úřad
IDS	Intrusion Detection System, systém pro odhalení průniku
IP adresa	Adresa, která jednoznačně číselně identifikuje počítač (síť) v internetu
IP	Internet Protokol
Malware	Malign software - škodlivý software
JE	Jaderná elektrárna
BIOS	Basic Input Output System – základní vstupně výstupní systém
OS	Operační Systém
PC	Personal Computer – osobní počítač
RAM	Random Access Memory – paměť s náhodným přístupem – typ paměti PC
MS	Microsoft – firma vyvíjející mimo jiné OS Windows
PWS	Password-stealing Trojan
DDoS	Distributed Denial of services – odepření služby

6 SEZNAM POUŽITÝCH OBRÁZKŮ

7 SEZNAM POUŽITÝCH GRAFŮ

8 SEZNAM POUŽITÝCH TABULEK

9 SEZNAM PŘÍLOH

Příloha 1- Dotazník

Průzkum informovanosti o hrozbách Internetu

Dobrý den, chtěl bych vás požádat o anonymní vyplnění dotazníku pro moji Bakalářskou práci, ve které se zaměřuji na hrozby, které ohrožují každého z nás kdo používáme internet. Test se skládá z 13 otázek a jeho vyplnění Vám zabere pouze několik minut.

Předem děkuji s pozdravem Lukáš Neuman.
Student FBMI ČVUT

Zadejte své údaje:

Pohlaví ----

Věk ----

Nejvyšší dosažené vzdělání Základní vzdělání

1. Jak často používáte počítač, tablet, mobilní telefon nebo nějaké jiné zařízení s přístupem k internetu?

- ☐ Téměř neustále
- ☐ Několik hodin denně
- ☐ Maximálně hodinu denně
- ☐ Několikrát do týdne

- [ ] Občas
- [ ] Vůbec

2. Za jak schopného se považujete při práci na PC?

- [ ] Začátečník (ovládám kancelářské programy, procházení internetu)
- [ ] Mírně Pokročilý (instalace programů)
- [ ] Pokročilý (nastavování aplikací, jednoduchá administrátorské úkoly)
- [ ] Profesionál (práce v příkazovém řádku, programování)

3. Používáte některé ze sociálních sítí? (prosím zaškrtněte všechny Vámi používané) (více možných odpovědí)

- [ ] Facebook
- [ ] Twitter
- [ ] Google+
- [ ] Jiné
- [ ] Žádné

4. Víte co to je Sociální inženýrství?

- [ ] Neslyšel jsem tento pojem

- [ ] Pojem jsem slyšel, ale nevím co znamená
- [ ] Ano, vím co pojem znamená
- [ ] Ano, setkal jsem se osobně se sociálním inženýrstvím

5. Víte co znamená pojem Phishing a setkali jste se s ním?

- [ ] Slyšel jsem o něm, ale nesetkal jsem se s ním
- [ ] Neslyšel jsem o něm a nevím, co to znamená
- [ ] Setkal jsem se s ním

6. Stalo se Vám, že Vám přišel email z banky nebo od provozovatele Vaší mailové schránky a žádal Vás o přihlášení?

- [ ] Ano
- [ ] Ne

7. Jaká byla Vaše reakce na tento email?

8. Jaká je Vaše reakce na neznámý email zřejmě reklamního charakteru?

- [ ] Smažu

- [ ] Označím jako spam
- [ ] Otevřu a přečtu si zprávu

9. Využíváte internet banking (případně bankovní aplikaci ve smartphonu)?

- [ ] Ano
- [ ] Ne

10. Jaký používáte antivirový program v PC?

- [ ] Avast
- [ ] AVG
- [ ] ESET
- [ ] Norton Security
- [ ] McAfee
- [ ] Jiný
- [ ] Žádný

11. Používáte nějaký antivirový program ve smartphonu nebo tabletu?

- [ ] Ano

- [ ] Ne

12. Setkali jste se ve svém počítači s virem?

- [ ] Ne
- [ ] Ano, jednou
- [ ] Ano, několikrát
- [ ] Nevím, nepoznám to

13. Jaký používáte Firewall?

- [ ] Integrovaný v operačním systému
- [ ] Žádný
- [ ] Nevím
- [ ] Jiný

14. Používáte různá hesla nebo jen jedno univerzálně všude?

- [ ] Ano, na různé účty mám různá hesla
- [ ] Ano, používám několik hesel, ale na některé účty jsou shodná
- [ ] Ne, používám pouze jedno heslo